NBG4115

Wireless N-lite 3G Home Router

User's Guide

Default Login Details

LAN IP Address	https://192.168.1.1
User Name	admin
Password	1234

Version 1.00
Edition 5, 4/2012

ZyXEL

www.zyxel.com

Copyright © 2012
ZyXEL Communications Corporation

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Graphics in this book may differ slightly from the product due to differences in operating systems, operating system versions, or if you installed updated firmware/software for your device. Every effort has been made to ensure that the information in this manual is accurate.

Related Documentation

- Quick Start Guide

  The Quick Start Guide shows how to connect the NBG4115 and configure it using the Web Configurator wizard.

Contents Overview

User's Guide 13

Introduction 15
ZyXEL NetUSB Share Center Utility 19
The Web Configurator 29
Connection Wizard 41
AP Mode 55
Tutorials 61

Technical Reference 75

Wireless LAN 77
WAN 97
LAN 113
DHCP Server 117
NAT 123
DDNS 133
Firewall 135
Content Filtering 139
Static Route 143
Bandwidth Management 146
Remote Management 154
UPnP 156
WoL 164
NetUSB 166
System 169
Logs 174
Tools 176
Sys OP Mode 181
Language 184
Troubleshooting 185

Table of Contents

Contents Overview **3**

Table of Contents **5**

Part I: User's Guide **13**

Chapter 1
Introduction **15**

1.1 Overview 15
1.2 Applications 15
1.3 Ways to Manage the NBG4115 15
1.4 Good Habits for Managing the NBG4115 16
1.5 LEDs 16
1.6 The WPS Button 17
1.7 Wall Mounting 18

Chapter 2
ZyXEL NetUSB Share Center Utility **19**

2.1 Overview 19
2.1.1 Quick Setup 20
2.1.2 Installing ZyXEL NetUSB Share Center Utility 20
2.2 The ZyXEL NetUSB Share Center Utility 21
2.2.1 The Menus 22
2.2.2 The Share Center Configuration Window 23
2.2.3 The Auto-Connect Printer List Window 24
2.3 Manually Connecting to USB Devices 24
2.4 Automatically Connecting to a USB Printer 26

Chapter 3
The Web Configurator **29**

3.1 Overview 29
3.2 Accessing the Web Configurator 29
3.3 Resetting the NBG4115 31
3.3.1 Procedure to Use the Reset Button 31
3.4 Navigating the Web Configurator 31
3.5 The Status Screen in Router Mode 31
3.5.1 Navigation Panel 35
3.5.2 Summary: DHCP Table 37

3.5.3 Summary: Packet Statistics 38
3.5.4 Summary: WLAN Station Status 38

Chapter 4
Connection Wizard 41

4.1 Overview 41
4.2 Wizard Setup 41
4.3 STEP 1: System Information 42
4.3.1 System Name 42
4.3.2 Domain Name 42
4.4 STEP 2: Wireless LAN 43
4.4.1 Extend (WPA-PSK or WPA2-PSK) Security 44
4.5 STEP 3: Internet Configuration 45
4.5.1 Ethernet Connection 46
4.5.2 PPPoE Connection 46
4.5.3 PPTP Connection 47
4.5.4 Mobile 3G 49
4.5.5 Your IP Address 50
4.5.6 WAN IP Address Assignment 50
4.5.7 IP Address and Subnet Mask 51
4.5.8 DNS Server Address Assignment 51
4.5.9 WAN IP and DNS Server Address Assignment 52
4.5.10 WAN MAC Address 53
4.6 Connection Wizard Complete 54

Chapter 5
AP Mode 55

5.1 Overview 55
5.2 Setting your NBG4115 to AP Mode 55
5.3 The Status Screen in AP Mode 56
5.3.1 Navigation Panel 58
5.4 LAN Settings 59
5.5 WLAN and Maintenance Settings 60
5.6 Logging in while in AP Mode 60

Chapter 6
Tutorials 61

6.1 Overview 61
6.2 Set Up a 3G Connection 61
6.3 Set Up the NBG4115 for Gaming 63
6.4 Set Up a Wireless Network with WPS 65
6.4.1 Push Button Configuration (PBC) 66
6.4.2 PIN Configuration 67

6.5 Configure Wireless Security without WPS 68
6.5.1 Configure Your Notebook 70
6.6 Bandwidth Management 71
6.6.1 Bandwidth Management by Application 71
6.6.2 Custom Bandwidth Management 72
6.6.3 Bandwidth Management by IP or IP Range 73

Part II: Technical Reference 75

Chapter 7
Wireless LAN 77

7.1 Overview 77
7.1.1 What You Can Do in this Chapter 77
7.1.2 What You Should Know 78
7.2 General 80
7.2.1 No Security 82
7.2.2 WEP Encryption 83
7.2.3 WPA-PSK/WPA2-PSK 85
7.3 MAC Filter 86
7.4 Advanced 87
7.5 QoS 89
7.5.1 Application Priority Configuration 90
7.6 WPS 92
7.7 WPS Station 93
7.8 Scheduling 94

Chapter 8
WAN 97

8.1 Overview 97
8.2 What You Can Do in this Chapter 97
8.2.1 What You Need To Know 98
8.3 The General Screen 100
8.4 The WAN1 Internet Connection Screen 102
8.4.1 Ethernet 103
8.4.2 PPPoE 104
8.4.3 PPTP 106
8.4.4 Mobile 3G 108
8.5 The Advanced Screen 110

Chapter 9
LAN 113

9.1 Overview 113
9.1.1 What You Can Do in this Chapter 113
9.2 What You Need To Know 113
9.3 IP 114

Chapter 10
DHCP Server 117

10.1 Overview 117
10.1.1 What You Can Do in this Chapter 117
10.1.2 What You Need To Know 117
10.2 General 118
10.3 Advanced 119
10.4 Client List 120

Chapter 11
NAT 123

11.1 Overview 123
11.1.1 What You Can Do in this Chapter 123
11.1.2 What You Need To Know 124
11.2 General 125
11.3 Application 126
11.4 Advanced 129
11.5 Technical Reference 130
11.5.1 NATPort Forwarding: Services and Port Numbers 130
11.5.2 NAT Port Forwarding Example 130
11.5.3 Trigger Port Forwarding 130
11.5.4 Trigger Port Forwarding Example 131
11.5.5 Two Points To Remember About Trigger Ports 131

Chapter 12
DDNS 133

12.1 Overview 133
12.2 General 133

Chapter 13
Firewall 135

13.1 Overview 135
13.1.1 What You Can Do in this Chapter 135
13.1.2 What You Need To Know 135
13.2 General 137
13.3 Services 137

Chapter 14
Content Filtering 139

14.1 Overview 139
14.1.1 What You Can Do in this Chapter 139
14.1.2 What You Need To Know 139
14.2 Filter 140
14.3 Technical Reference 141
14.3.1 Customizing Keyword Blocking URL Checking 141

Chapter 15
Static Route 143

15.1 Overview 143
15.1.1 What You Can Do in this Chapter 143
15.2 IP Static Route 144
15.2.1 Static Route Setup Screen 145

Chapter 16
Bandwidth Management 146

16.1 Overview 146
16.1.1 What You Can Do in this Chapter 146
16.1.2 What You Need To Know 146
16.2 General 147
16.3 Advanced 148
16.3.1 Pre-Configured Gaming Ports 151
16.3.2 Priority Levels 151
16.3.3 User Defined Service Rule Configuration 151
16.3.4 Predefined Bandwidth Management Services 152
16.3.5 Services and Port Numbers 153

Chapter 17
Remote Management 154

17.1 Overview 154
17.1.1 What You Can Do in this Chapter 154
17.1.2 What You Need To Know 154
17.2 WWW 155

Chapter 18
UPnP 156

18.1 Overview 156
18.1.1 What You Can Do in this Chapter 156
18.1.2 What You Need to Know 156
18.2 General 157
18.3 Technical Reference 158
18.3.1 Installing UPnP in Windows XP 158

Chapter 19
WoL 164

19.1 Overview 164
19.1.1 What You Can Do in this Chapter 164
19.2 The WoL General Screen 164

Chapter 20
NetUSB 166

20.1 Overview 166
20.1.1 What You Can Do in this Chapter 166
20.1.2 What You Need to Know 166
20.2 The NetUSB General Screen 167

Chapter 21
System 169

21.1 Overview 169
21.1.1 What You Can Do in this Chapter 169
21.2 General 169
21.3 Time Setting 171

Chapter 22
Logs 174

22.1 Overview 174
22.1.1 What You Can Do in this Chapter 174
22.2 View Log 174

Chapter 23
Tools 176

23.1 Overview 176
23.1.1 What You Can Do in this Chapter 176
23.2 Firmware 176
23.3 Configuration 178
23.3.1 Backup Configuration 178
23.3.2 Restore Configuration 178
23.3.3 Back to Factory Defaults 179
23.4 Restart 180

Chapter 24
Sys OP Mode 181

24.1 Overview 181
24.1.1 What You Can Do in this Chapter 181
24.1.2 What You Need to Know 181
24.2 General 182

Chapter 25
Language 184

25.1 Overview 184
25.2 Language 184

Chapter 26
Troubleshooting 185

26.1 Overview 185
26.2 Power, Hardware Connections, and LEDs 185
26.3 NBG4115 Access and Login 186
26.4 Internet Access 188
26.5 Resetting the NBG4115 to Its Factory Defaults 189
26.6 Wireless Router/AP Troubleshooting 189
26.7 ZyXEL NetUSB Share Center Utility Problems 190

Appendix A Pop-up Windows, JavaScripts and Java Permissions 193

Appendix B IP Addresses and Subnetting 205

Appendix C Setting Up Your Computer's IP Address 215

Appendix D Wireless LANs 243

Appendix E Common Services 257

Appendix F Legal Information 261

Index 269

PART I
User's Guide

1 Introduction

1.1 Overview

This chapter introduces the main features and applications of the NBG4115.

The NBG4115 extends the range of your existing wired network without additional wiring, providing easy network access to mobile users. You can set up a wireless network with other IEEE 802.11b/g/n compatible devices.

A range of services such as a firewall and content filtering are also available for secure Internet computing.

Note: Be sure to install the Share Center Utility (for NetUSB™ functionality) from the included disc, or download the latest version from the zyxel.com website.

1.2 Applications

Your can create the following networks using the NBG4115:

- **Wired**. You can connect network devices via the Ethernet ports of the NBG4115 so that they can communicate with each other and access the Internet.
- **Wireless**. Wireless clients can connect to the NBG4115 to access network resources.
- **WAN**. Connect to a broadband modem/router for Internet access.
- **WPS**. Create an instant network connection with another WPS-compatabile device, sharing your network connection with it.
- **3G Wireless**. Connect to a local 3G wireless network to take advantage of superior connection speeds and improved download times.
- **NetUSB**. The NBG4115 allows you to connect a USB device (such as printer, scanner, or portable hard disk) directly to the USB port and then share that device over the Internet. You can also connect a USB to the NBG4115, which can then share up to 3 additional USB devices with the rest of your personal home network.

1.3 Ways to Manage the NBG4115

Use any of the following methods to manage the NBG4115.

- WPS (Wi-Fi Protected Setup). You can use the WPS button or the WPS section of the Web Configurator to set up a wireless network with your ZyXEL Device.

- Web Configurator. This is recommended for everyday management of the NBG4115 using a (supported) web browser.

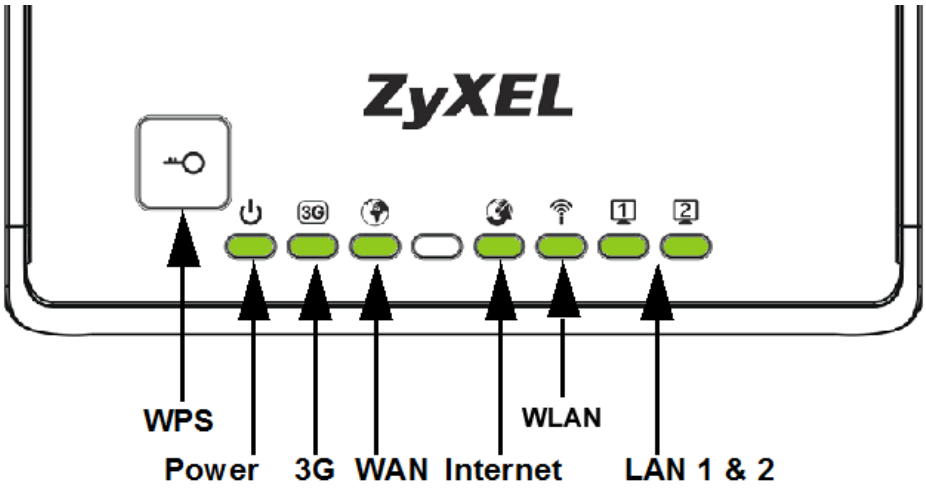
1.4 Good Habits for Managing the NBG4115

Do the following things regularly to make the NBG4115 more secure and to manage the NBG4115 more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the NBG4115 to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the NBG4115. You could simply restore your last configuration.

1.5 LEDs

Figure 1 Front Panel



The following table describes the LEDs and the WPS button.

Table 1 Front Panel LEDs and WPS Button

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The NBG4115 is receiving power and functioning properly.
		Off	The NBG4115 is not receiving power.

Table 1 Front Panel LEDs and WPS Button

LED	COLOR	STATUS	DESCRIPTION
WLAN	Green	On	The NBG4115 is ready, but is not sending/receiving data through the wireless LAN.
		Blinking	The NBG4115 is sending/receiving data through the wireless LAN. The NBG4115 is negotiating a WPS connection with a wireless client.
		Off	The wireless LAN is not ready or has failed.
WAN	Green	On	The NBG4115 has a successful 10/100MB WAN connection.
		Blinking	The NBG4115 is sending/receiving data through the WAN.
		Off	The WAN connection is not ready, or has failed.
LAN 1-2	Green	On	The NBG4115 has a successful 10/100MB Ethernet connection.
		Blinking	The NBG4115 is sending/receiving data through the LAN.
		Off	The LAN is not connected.
3G	Green	On	The NBG4115 has a 3G card installed and is communicating with routers.
		Blinking	The NBG4115 is transmitting and/or receiving data from routers through an installed 3G card.
		Off	There is no 3G card installed.
Internet	Green	On	The NBG4115 has received an IP address through either the WAN or WLAN interface and can connect to the Internet.
		Off	The NBG4115 has not received an IP address through either the WAN or WLAN interface and as such cannot connect to the Internet.
WPS Button	Press this button for 1 second to set up a wireless connection via WiFi Protected Setup with another WPS-enabled client. You must press the WPS button on the client side within 120 seconds for a successful connection.		

1.6 The WPS Button

Your NBG4115 supports WiFi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the WiFi Alliance.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Each WPS connection works between two devices. Both devices must support WPS (check each device's documentation to make sure).

Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has two minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

For more information on using WPS, see Section 6.4 on page 65.

1.7 Wall Mounting

You may need screw anchors if mounting on a concrete or brick wall.

Table 2 Wall Mounting Information

Distance between holes	8.8 cm
M4 Screws	Two
Screw anchors (optional)	Two

1 Select a position free of obstructions on a wall strong enough to hold the weight of the device.

2 Mark two holes on the wall at the appropriate distance apart for the screws.

Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.

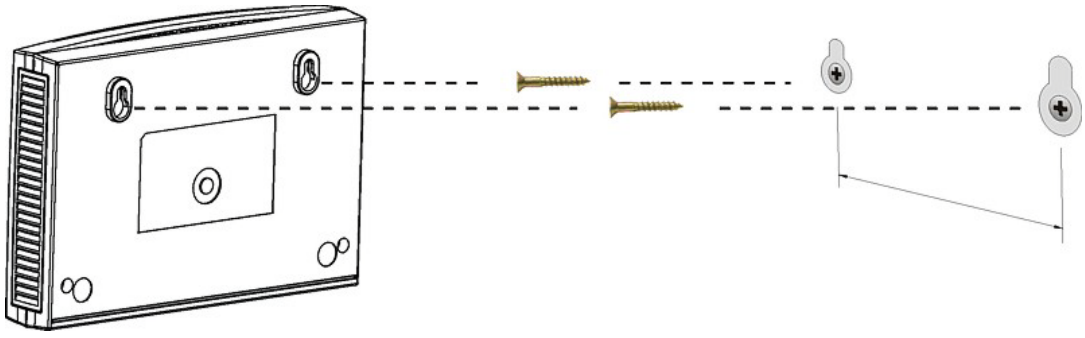
3 If using screw anchors, drill two holes for the screw anchors into the wall. Push the anchors into the full depth of the holes, then insert the screws into the anchors. Do not insert the screws all the way in - leave a small gap of about 0.5 cm.

If not using screw anchors, use a screwdriver to insert the screws into the wall. Do not insert the screws all the way in - leave a gap of about 0.5 cm.

4 Make sure the screws are fastened well enough to hold the weight of the NBG4115 with the connection cables.

5 Align the holes on the back of the NBG4115 with the screws on the wall. Hang the NBG4115 on the screws.

Figure 2 Wall Mounting Example



2

ZyXEL NetUSB Share Center Utility

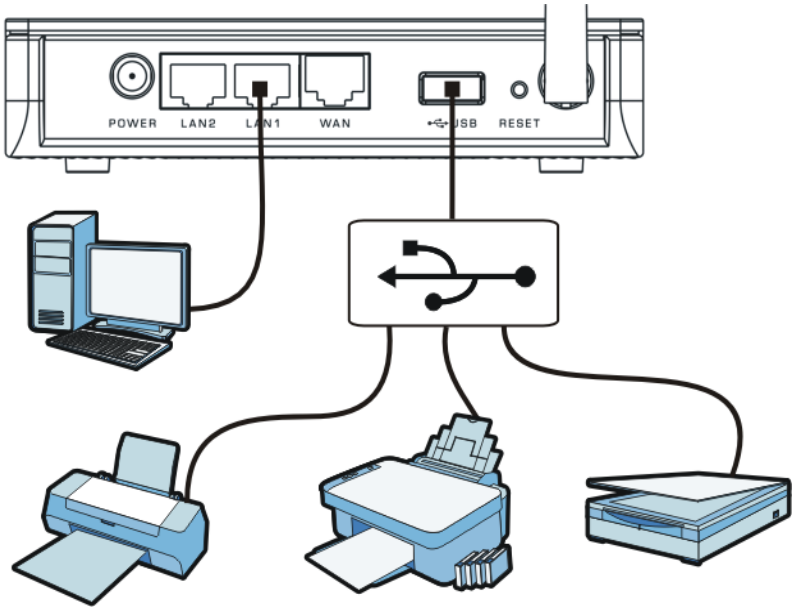
2.1 Overview

The ZyXEL NetUSB Share Center Utility allows you to work with the USB devices that are connected directly to the NBG4115 as if they are connected directly to your computer. This allows you to easily share USB-based devices such as printers, scanners, portable hard disks, MP3 players, faxes, and digital cameras (to name a few) with all the other people in your home or office as long as they are connected to the NBG4115 and have the ZyXEL NetUSB Share Center Utility installed.

For information on configuring the USB network sharing function in the Web Configurator, see Chapter 20 on page 166.

Note: Be sure to install the Share Center Utility (for NetUSB functionality) from the included disc, or download the latest version from the zyxel.com website.

Figure 3 Example of NetUSB



In this example, a USB printer, digital camera, and scanner are all connected to a USB hub. The hub is in turn connected directly to the NBG4115. Any computer with a ZyXEL NetUSB Share Center Utility installed on it and which is connected to the NBG4115's LAN ports can access these devices.

Note: A USB hub attached to the NBG4115 requires its own power adapter.

2.1.1 Quick Setup

This section shows you how to get started using the ZyXEL NetUSB Share Center Utility.

1 Install the ZyXEL NetUSB Share Center Utility on each computer connected to the NBG4115.

2 Connect a USB device to the USB port on the NBG4115.

Note: If you are connecting multiple devices to the NBG4115, first connect a USB hub to the NBG4115 then connect your other USB devices to it.

3 Run the ZyXEL NetUSB Share Center Utility to display a list of all connected USB devices, then use it to connect your computer to them.

2.1.2 Installing ZyXEL NetUSB Share Center Utility

Before you can access USB devices connected to the NBG4115, you must first install the ZyXEL NetUSB Share Center Utility on any computer on your LAN to which you want to allow access to these devices.

Note: In order to properly use the ZyXEL NetUSB Share Center Utility with your NBG4115, ensure that the NBG4115 firmware is version v1.00(BFS.3) or higher. See Chapter 23 on page 176 for information on updating your device's firmware.

To install the ZyXEL NetUSB Share Center Utility:

1 Insert the disc that came with your NBG4115 into your computer's disc drive.

2 Run the **Setup** program by double-clicking it and then follow the on-screen instructions for installing it on your computer.

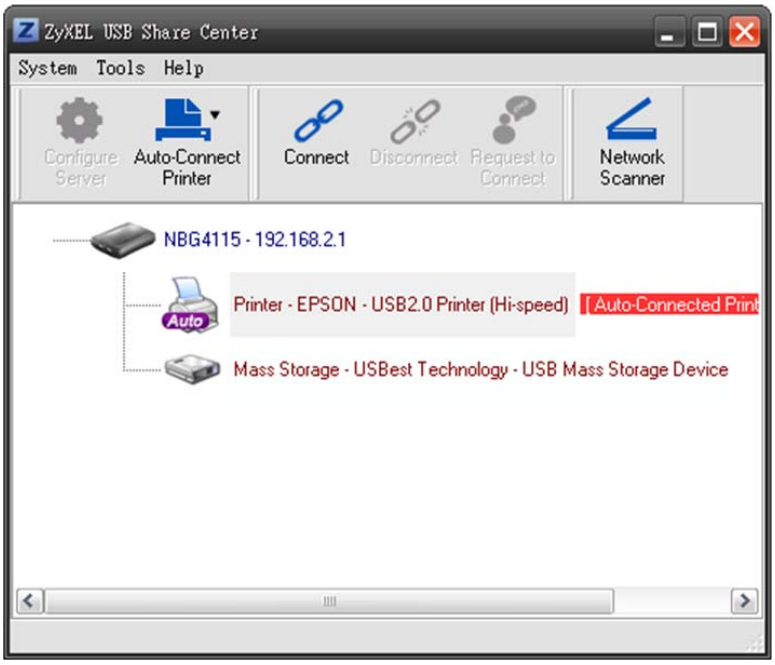
Note: The following operating systems are supported: Windows XP/Vista/7 (32 and 64-bit versions), Mac OS X 10.4, 10.5 and 10.6.

3 To open the ZyXEL NetUSB Share Center Utility double-click its system tray icon.

2.2 The ZyXEL NetUSB Share Center Utility

This section describes the ZyXEL NetUSB Share Center Utility main window.

Figure 4 ZyXEL NetUSB Share Center Utility Main Window



The following table describes the icons in this window.

Table 3 ZyXEL NetUSB Share Center Utility Main Window Icons

ICON	DESCRIPTION
	Configure Server Click to open the NBG4115's built-in Web Configurator, which you can use to set up the NBG4115 (see Chapter 3 on page 29 for details).
	Auto-Connect Printer Click this if you want to automatically connect to the printer each time your start your computer. Note: You must first install the appropriate print driver on each computer for which you intend to use this feature. See the documentation that came with your printer for instructions on how to do this.
	Connect Select a USB device and then click this button to connect to it. Your computer can connect to as many USB devices as are connected to the NBG4115.
	Disconnect Select a device to which your computer is connected and then click this button to disconnect from it.

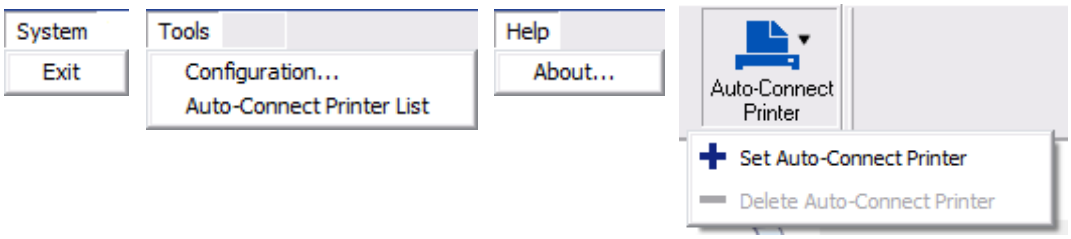
Table 3 ZyXEL NetUSB Share Center Utility Main Window Icons (continued)

ICON	DESCRIPTION
	Request to Connect Some USB devices may not allow automatic connections over the network. If so, select the device in question and click this button to issue a request to connect to it.
	Network Scanner Click this to open the scanner options on your computer for working with a scanner connected to the network.

2.2.1 The Menus

This section describes the utility's menus.

Figure 5 ZyXEL NetUSB Share Center Utility Menus



The following table describes the menus in this screen.

Table 4 ZyXEL NetUSB Share Center Utility Main Screen Menus

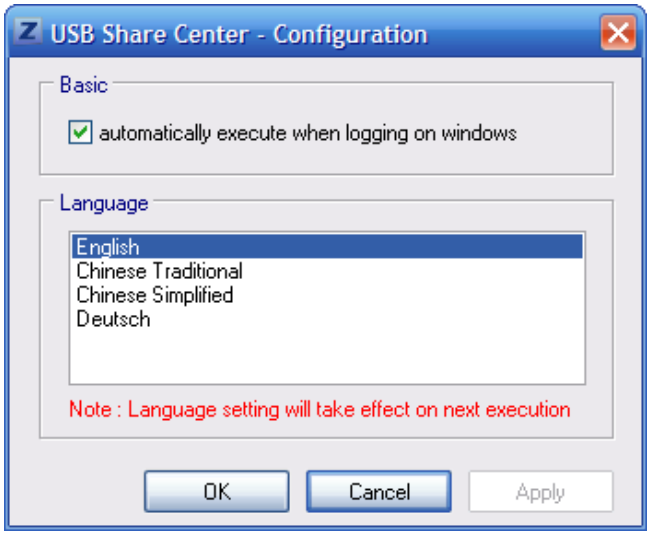
MENU	ITEM	DESCRIPTION
System	Exit	This closes the ZyXEL NetUSB Share Center Utility.
Tools	Configuration	This opens the ZyXEL NetUSB Share Center Utility configuration window.
	Auto-Connect Printer List	This opens the list window that displays all of the printing devices connected to the NBG4115.
Help	About	This opens the about window, which provides information of the utility software and driver versions.
Auto-Connect Printer	Set Auto-Connect Printer	This sets the selected printer to 'auto-connect', meaning your computer will always connect to the printer over the network. Note: You first must install the appropriate drivers for the printer that you intend to use.
	Delete Auto-Connect Printer	This removes the auto-connect option from the selected printer.

2.2.2 The Share Center Configuration Window

This section describes the utility's configuration window, which allows you to set certain options for the utility. These options do not apply to the USB devices connected to the NBG4115.

You can open it by clicking the **Tools > Configuration** menu command.

Figure 6 ZyXEL NetUSB Share Center Utility Configuration Window



The following table describes the labels in this window.

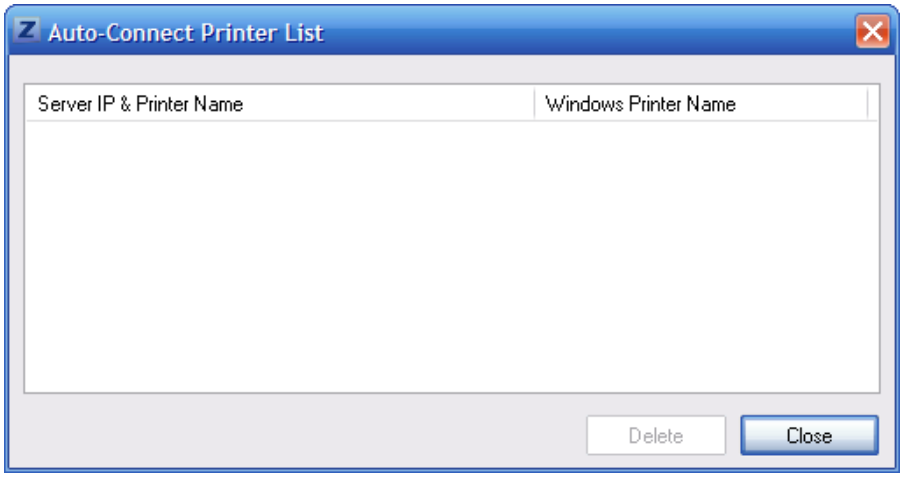
Table 5 ZyXEL NetUSB Share Center Utility Configuration Window

LABEL	DESCRIPTION
Basic	Select this to run the utilty automatically when you log into or start up Windows.
Language	Select a language for the ZyXEL NetUSB Share Center Utility. You must restart the utility for the change to take effect.
OK	Click this to save your changes and close the window.
Cancel	Click this cancel to close the window without saving.
Apply	Click this to save your changes without closing the window.

2.2.3 The Auto-Connect Printer List Window

This section describes the utility's auto-connect printer list window. You can open it by clicking the **Tools > Auto-Connect Printer List** menu command.

Figure 7 ZyXEL NetUSB Share Center Utility Auto-Connect Printer List Window



The following table describes the labels in this screen.

Table 6 ZyXEL NetUSB Share Center Utility Auto-Connect Printer List Window

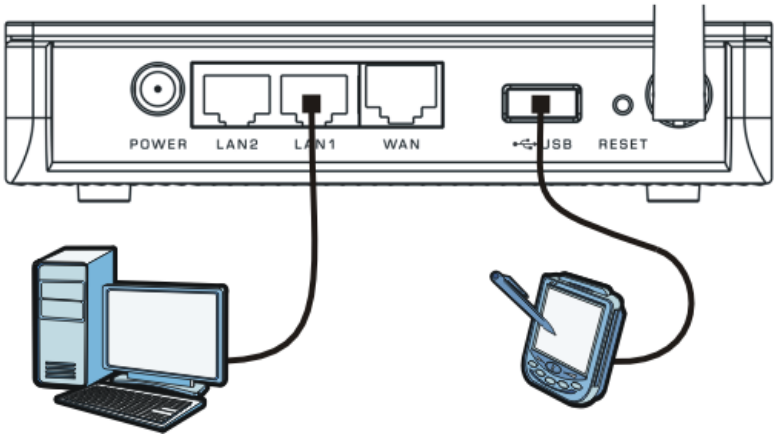
LABEL	DESCRIPTION
Server IP & Printer Name	Displays a list of print server IPs and printer names connected to this NBG4115.
Windows Printer Name	Displays a corresponding list of Windows printer names connected to this devices listed in the other list.
Delete	Select an printer from the list and click this to remove it.
Close	Click this to close the window.

2.3 Manually Connecting to USB Devices

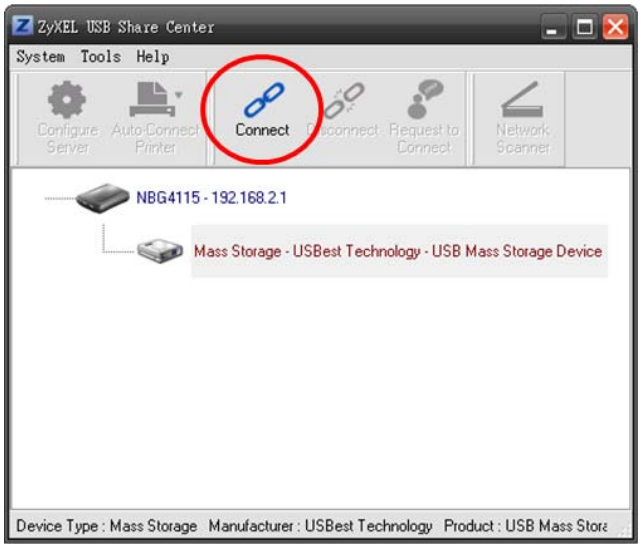
This example shows you how to connect to a USB device over your NBG4115 network. Makes sure that you have first installed the ZyXEL NetUSB Share Center Utility on the computer to which you want to connect the USB devices.

Note: If you do this with a USB printer but do not yet have the print driver installed you will be prompted to install one by the Windows New Hardware Wizard.

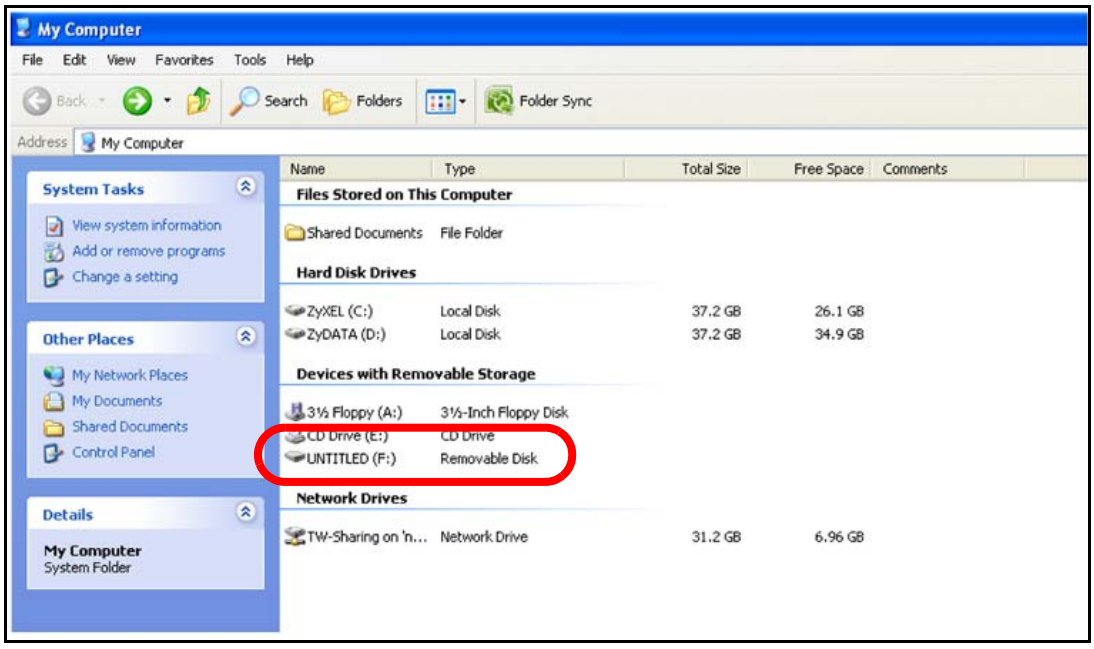
1 Connect a USB device to the NBG4115.



2 In the **ZyXEL NetUSB Share Center Utility**, select the device and click **Connect**.



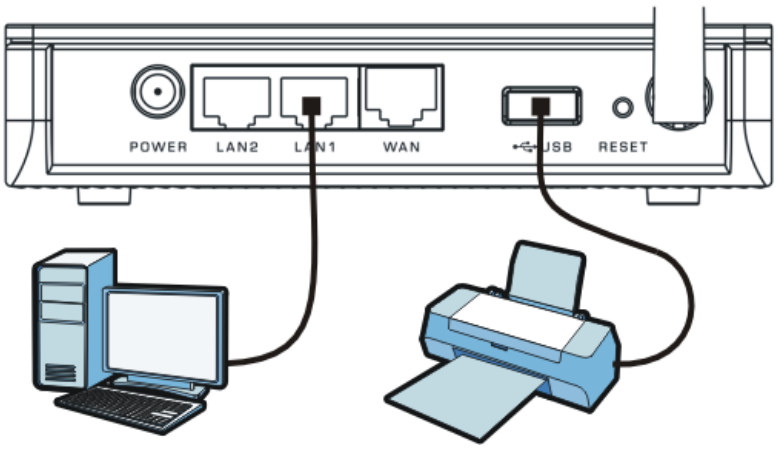
3 The device mounts on your system.



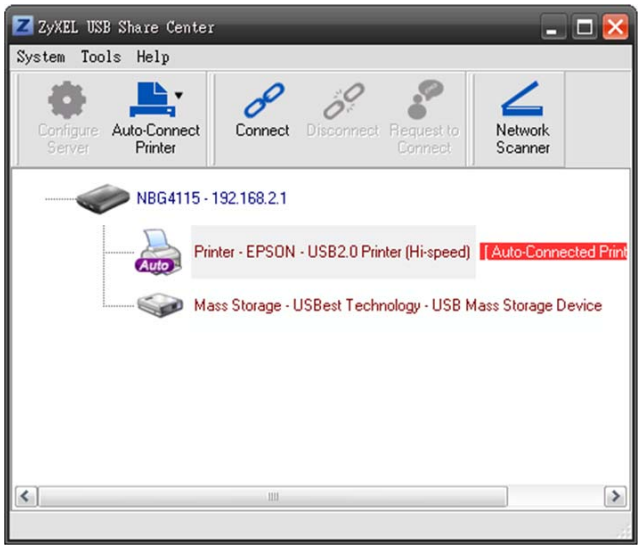
2.4 Automatically Connecting to a USB Printer

This example shows you how to set your computer to automatically connect to a shared USB printer over your NBG4115 network each time you log into your computer. Makes sure that you have first installed the ZyXEL NetUSB Share Center Utility.

1 Connect a USB printer to the NBG4115.



2 Open the **ZyXEL Sharing Center Utility** on the computer that you want to use to connect to the printer.



Click the **Connect** button. You may be prompted to install a printer driver or to configure other settings.

3 Finally, click the **Auto-Connect Printer** menu and select **Set Auto-Connect Printer** from the menu.

3

The Web Configurator

3.1 Overview

This chapter describes how to access the NBG4115 Web Configurator and provides an overview of its screens.

The Web Configurator is an HTML-based management interface that allows easy setup and management of the NBG4115 via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions or Safari 2.0 or later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the Web Configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Refer to the Troubleshooting chapter to see how to make sure these functions are allowed in Internet Explorer.

3.2 Accessing the Web Configurator

1. Make sure your NBG4115 hardware is properly connected and prepare your computer or computer network to connect to the NBG4115 (refer to the Quick Start Guide).
2. Launch your web browser.
3. Type "http://192.168.1.1" as the website address.

   Your computer must be in the same subnet in order to access this website address.
4. Type "1234" (default) as the password and click **Login**. In some versions, the default password appears automatically - if this is the case, click **Login**.

5 You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password (and retype it to confirm) and click **Apply** or click **Ignore**.

Figure 8 Change Password Screen

ZyXEL
Please enter a new password
Your router is currently using the default password. To protect your network from unauthorized users we suggest you change your password at this time. Please select a new password that will be easy to remember yet difficult for others to guess.We suggest you combine text with numbers to make it more difficult for an intruder to guess.
The administrator password should must be between 1 - 30 characters.
New Password:
****
Retype to Confirm:
Apply
Ignore

Note: The management session automatically times out when the time period set in the **Administrator Inactivity Timer** field expires (default five minutes). Simply log back into the NBG4115 if this happens.

6 Select the setup mode you want to use.

- Click **Go to Wizard Setup** to use the Configuration Wizard for basic Internet and Wireless setup.
- Click **Go to Advanced Setup** to view and configure all the NBG4115's settings.
- Select a language to go to the basic Web Configurator in that language. To change to the advanced configurator see Chapter 25 on page 184.

Figure 9 Selecting the setup mode

ZyXEL
Please select Wizard or Advanced mode
The Wizard setup walks you through the most common configuration settings. We suggest you use this mode if it is the first time you are setting up your device.
Use Advanced mode if you need access to more advanced features.
Go to Wizard setup
Go to Advanced setup
Choose your language below
English
Deutsch
Français
Español
繁體中文
Italiano
簡体中文
Exit

3.3 Resetting the NBG4115

If you forget your password or IP address, or you cannot access the Web Configurator, you will need to use the **RESET** button at the back of the NBG4115 to reload the factory-default configuration file. This means that you will lose all configurations that you had previously saved, the password will be reset to "1234" and the IP address will be reset to "192.168.1.1".

3.3.1 Procedure to Use the Reset Button

1. Make sure the power LED is on.
2. Press the **RESET** button for longer than 1 second to restart/reboot the NBG4115.
3. Press the **RESET** button for longer than five seconds to set the NBG4115 back to its factory-default configurations.

3.4 Navigating the Web Configurator

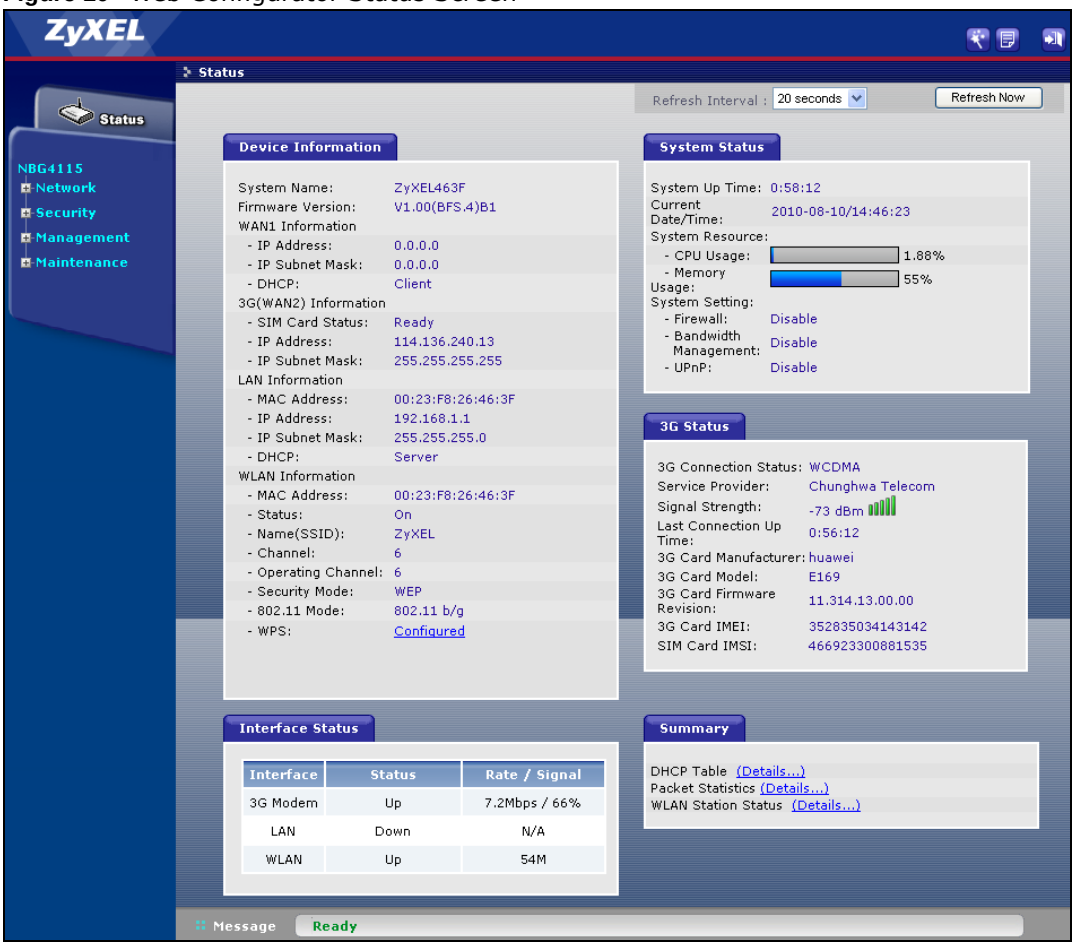
The following summarizes how to navigate the Web Configurator from the **Status** screen in **Router Mode** and **AP Mode**.

3.5 The Status Screen in Router Mode

Click on **Status**. The screen below shows the status screen in **Router Mode**.

(For information on the status screen in **AP Mode** see Chapter 5 on page 56.)

Figure 10 Web Configurator Status Screen



The following table describes the icons shown in the **Status** screen.

Table 7 Status Screen Icon Key

ICON	DESCRIPTION
	Click this icon to open the setup wizard.
	Click this icon to view copyright and a link for related product information.
	Click this icon at any time to exit the Web Configurator.
	Select a number of seconds or **None** from the drop-down list box to refresh all screen statistics automatically at the end of every time interval or to not refresh the screen statistics.
	Click this button to refresh the status screen statistics.

The following table describes the labels shown in the **Status** screen.

Table 8 Web Configurator Status Screen

LABEL	DESCRIPTION
Device Information	
System Name	This is the **System Name** you enter in the **Maintenance** > **System** > **General** screen. It is for identification purposes.
Firmware Version	This is the firmware version and the date created.
WAN Information	
- SIM Card Status	(3G Only) When a 3G USB device is attached to the NBG4115, this provides information specific to it.
- MAC Address	This shows the WAN Ethernet adapter MAC Address of your device.
- IP Address	This shows the WAN port's IP address.
- IP Subnet Mask	This shows the WAN port's subnet mask.
- DHCP	This shows the WAN port's DHCP role - **Client** or **None**.
LAN Information	
- MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
- IP Address	This shows the LAN port's IP address.
- IP Subnet Mask	This shows the LAN port's subnet mask.
- DHCP	This shows the LAN port's DHCP role - **Server** or **None**.
WLAN Information	
- MAC Address	This shows the wireless adapter MAC Address of your device.
- Status	This shows the current status of the Wireless LAN - **On**, **Off** or **Off by scheduler**.
- Name (SSID)	This shows a descriptive name used to identify the NBG4115 in the wireless LAN.
- Channel	This shows the channel number which you select manually.
- Operating Channel	This shows the channel number which the NBG4115 is currently using over the wireless LAN.
- Security Mode	This shows the level of wireless security the NBG4115 is using.
- 802.11 Mode	This shows the wireless standard.
- WPS	This displays **Configured** when the WPS has been set up. This displays **Unconfigured** if the WPS has not been set up. Click the status to display Network > Wireless LAN > WPS screen.
System Status	
System Up Time	This is the total time the NBG4115 has been on.
Current Date/Time	This field displays your NBG4115's present date and time.
System Resource	
- CPU Usage	This displays what percentage of the NBG4115's processing ability is currently used. When this percentage is close to 100%, the NBG4115 is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications.
- Memory Usage	This shows what percentage of the heap memory the NBG4115 is using.
System Setting	
- Firewall	This shows whether the firewall is active or not.
- Bandwidth Management	This shows whether bandwidth management is enabled or not.
- UPnP	This shows whether UPnP is active or not.

Table 8 Web Configurator Status Screen (continued)

LABEL	DESCRIPTION
3G Status This section displays only when you select the **Fixed 3G Router Mode** option in the **NetUSB > General** screen and/or attach a 3G USB dongle to the USB port.	
3G Connection Status	This displays the type of the 3G network (such as **WCDMA**) to which the NBG4115 is connected when the 3G connection is up or **No Service** when the 3G connection is down or not activated.
Service Provider	This displays the name of your network service provider.
Signal Strength	This displays the strength of the signal. The signal strength mainly depends on the antenna output power and the distance between your NBG4115 and the service provider's base station. You can see a signal strength indication even when the NBG4115 does not have a 3G connection (because the signal is still there even when the NBG4115 is not using it).
Last Connection Up Time	This displays how long the 3G connection has been up.
3G Card Manufacturer	This displays the manufacturer of your 3G card.
3G Card Model	This displays the model name of your 3G card.
3G Card Firmware Revision	This displays the version of the firmware currently used in the 3G card.
3G Card IMEI	This displays the International Mobile Equipment Number (IMEI) which is the serial number of the 3G wireless card. IMEI is a unique 15-digit number used to identify a mobile device.
SIM Card IMSI	This displays the International Mobile Subscriber Identity (IMSI) stored in the SIM (Subscriber Identity Module) card. The SIM card is installed in a mobile device and used for authenticating a customer to the carrier network. IMSI is a unique 15-digit number used to identify a user on a network.
Interface Status	
Interface	This displays the NBG4115 port types. The port types are: **WAN** or **3G Modem**, **LAN** and **WLAN**.
Status	For the 3G, LAN and WAN ports, this field displays **Down** (line is down) or **Up** (line is up or connected). For the WLAN, it displays **Up** when the WLAN is enabled or **Down** when the WLAN is disabled.
Rate Rate / Signal	For the LAN ports, this displays the port speed and duplex setting or **N/A** when the line is disconnected. For the WAN port, it displays the port speed and duplex setting if you're using Ethernet encapsulation and **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) and **Drop** (dropping a call) if you're using PPPoE or PPTP encapsulation. This field displays **N/A** when the line is disconnected. For the 3G port, it displays the current data rate if the 3G connection is up and **N/A** when the 3G connection is down. It also displays the strength of the signal. For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and **N/A** when the WLAN is disabled.
Summary	
DHCP Table	Use this screen to view current DHCP client information.
Packet Statistics	Use this screen to view port status and packet specific statistics.
WLAN Station Status	Use this screen to view the wireless stations that are currently associated to the NBG4115.

3.5.1 Navigation Panel

Use the sub-menus on the navigation panel to configure NBG4115 features.

The following table describes the sub-menus.

Table 9 Screens Summary

LINK	TAB	FUNCTION
Status		This screen shows the NBG4115's general device, system and interface status information. Use this screen to access the wizard, and summary statistics tables.
Network		
Wireless LAN	General	Use this screen to configure wireless LAN.
	MAC Filter	Use the MAC filter screen to configure the NBG4115 to block access to devices or block the devices from accessing the NBG4115.
	Advanced	This screen allows you to configure advanced wireless settings.
	QoS	Use this screen to configure Wi-Fi Multimedia Quality of Service (WMM QoS). WMM QoS allows you to prioritize wireless traffic according to the delivery requirements of individual services.
	WPS	Use this screen to configure WPS.
	WPS Station	Use this screen to add a wireless station using WPS.
	Scheduling	Use this screen to schedule the times the Wireless LAN is enabled.
WAN	Internet Connection	This screen is not available when you select the **Fixed 3G Router Mode** option in the **NetUSB > General** screen. Use this screen to configure ISP parameters, WAN IP address assignment, DNS servers and the WAN MAC address.
	General	This screen is available only when you select the **Fixed 3G Router Mode** option in the **NetUSB > General** screen. Use this screen to configure WAN priority, the action the NBG4115 takes after the primary WAN interface fails, and connection test settings.
	WAN1	This screen is available only when you select the **Fixed 3G Router Mode** option in the **NetUSB > General** screen. Use this screen to configure the WAN1 connection for Internet access.
	3G(WAN2)	This screen is available only when you select the **Fixed 3G Router Mode** option in the **NetUSB > General** screen. Use this screen to configure the 3G WAN2 connection for Internet access.
	Advanced	Use this screen to configure other advanced properties.
LAN	IP	Use this screen to configure LAN IP address and subnet mask.

Table 9 Screens Summary

LINK	TAB	FUNCTION
DHCP Server	General	Use this screen to enable the NBG4115's DHCP server.
	Advanced	Use this screen to assign IP addresses to specific individual computers based on their MAC addresses and to have DNS servers assigned by the DHCP server.
	Client List	Use this screen to view current DHCP client information and to always assign an IP address to a MAC address (and host name).
NAT	General	Use this screen to enable NAT.
	Application	Use this screen to configure servers behind the NBG4115.
	Advanced	Use this screen to change your NBG4115's port triggering settings.
DDNS	General	Use this screen to set up dynamic DNS.
Security		
Firewall	General	Use this screen to activate/deactivate the firewall.
	Services	This screen shows a summary of the firewall rules, and allows you to edit/add a firewall rule.
Content Filter	Filter	Use this screen to block certain web features and sites containing certain keywords in the URL.
Management		
Static Route	IP Static Route	Use this screen to configure IP static routes.
Bandwidth Management	General	Use this screen to use pre-configured bandwidth management profiles for how your NBG4115 manages incoming and outgoing data.
	Advanced	Use this screen to create your own bandwidth management profile for how your NBG4115 manages incoming and outgoing data.
Remote MGMT	WWW	Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTP to manage the NBG4115.
UPnP	General	Use this screen to enable UPnP on the NBG4115.
WOL	General	Use this screen to enable Wake on LAN to remotely turn on a device on the local network.
NetUSB	General	Use this screen to configure how the NBG4115 uses 3G wireless access.
Maintenance		
System	General	Use this screen to view and change administrative settings such as system and domain names, password and inactivity timer.
	Time Setting	Use this screen to change your NBG4115's time and date.
Logs	View Log	Use this screen to view the logs for the categories that you selected.
Tools	Firmware	Use this screen to upload firmware to your NBG4115.
	Configuration	Use this screen to backup and restore the configuration or reset the factory defaults to your NBG4115.
	Restart	This screen allows you to reboot the NBG4115 without turning the power off.

Table 9 Screens Summary

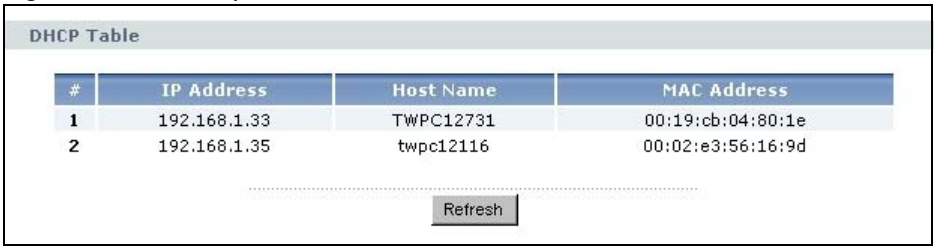
LINK	TAB	FUNCTION
Sys OP Mode	General	This screen allows you to select whether your device acts as a Router or a Access Point.
Language	Language	This screen allows you to select the language you prefer.

3.5.2 Summary: DHCP Table

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the NBG4115's LAN as a DHCP server or disable it. When configured as a server, the NBG4115 provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on that network, or else the computer must be manually configured.

Click the **DHCP Table (Details...)** hyperlink in the **Status** screen. Read-only information here relates to your DHCP status. The DHCP table shows current DHCP client information (including **IP Address**, **Host Name** and **MAC Address**) of all network clients using the NBG4115's DHCP server.

Figure 11 Summary: DHCP Table



The following table describes the labels in this screen.

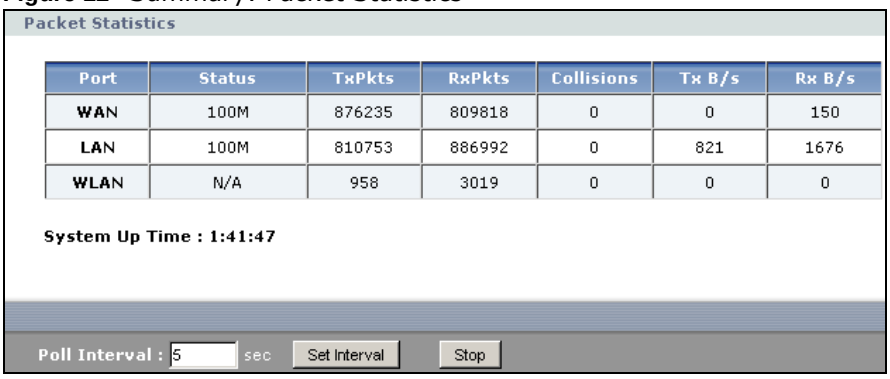
Table 10 Summary: DHCP Table

LABEL	DESCRIPTION
#	This is the index number of the host computer.
IP Address	This field displays the IP address relative to the # field listed above.
Host Name	This field displays the computer host name.
MAC Address	This field shows the MAC address of the computer with the name in the **Host Name** field. Every Ethernet device has a unique MAC (Media Access Control) address which uniquely identifies a device. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
Refresh	Click **Refresh** to renew the screen.

3.5.3 Summary: Packet Statistics

Click the **Packet Statistics (Details...)** hyperlink in the **Status** screen. Read-only information here includes port status, packet specific statistics and the "system up time". The **Poll Interval(s)** field is configurable and is used for refreshing the screen.

Figure 12 Summary: Packet Statistics



The following table describes the labels in this screen.

Table 11 Summary: Packet Statistics

LABEL	DESCRIPTION
Port	This is the NBG4115's port type.
Status	For the LAN ports, this displays the port speed and duplex setting or **Down** when the line is disconnected. For the WAN port, it displays the port speed and duplex setting if you're using Ethernet encapsulation and **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) and **Drop** (dropping a call) if you're using PPPoE or PPTP encapsulation. This field displays **Down** when the line is disconnected. For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and **Down** when the WLAN is disabled.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.
Collisions	This is the number of collisions on this port.
Tx B/s	This displays the transmission speed in bytes per second on this port.
Rx B/s	This displays the reception speed in bytes per second on this port.
System Up Time	This is the total time the NBG4115 has been on.
Poll Interval(s)	Enter the time interval for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the **Poll Interval(s)** field.
Stop	Click **Stop** to stop refreshing statistics.

3.5.4 Summary: WLAN Station Status

Click the **WLAN Station Status (Details...)** hyperlink in the **Status** screen. View the wireless stations that are currently associated to the NBG4115 in the **Association List**. Association means that a wireless client (for example, your network or computer with a wireless network card) has

connected successfully to the AP (or wireless router) using the same SSID, channel and security settings.

Figure 13 Summary: Wireless Association List

The following table describes the labels in this screen.

Table 12 Summary: Wireless Association List

LABEL	DESCRIPTION
#	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC address of an associated wireless station.
Association Time	This field displays the time a wireless station first associated with the NBG4115's WLAN network.
Refresh	Click **Refresh** to reload the list.

4

Connection Wizard

4.1 Overview

This chapter provides information on the wizard setup screens in the Web Configurator.

4.2 Wizard Setup

The Web Configurator's wizard setup helps you configure your device to access the Internet. Refer to your ISP (Internet Service Provider) checklist in the Quick Start Guide to know what to enter in each field. Leave a field blank if you don't have that information.

1 After you access the NBG4115 Web Configurator, click the **Go to Wizard setup** hyperlink.

You can click **Go to Advanced setup** hyperlink to skip this wizard setup and configure basic or advanced features accordingly.

Figure 14 Select Wizard or Advanced Mode

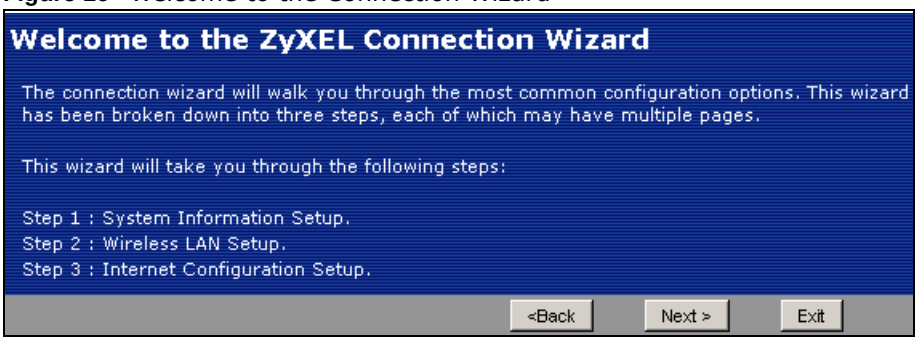
ZyXEL
Please select Wizard or Advanced mode
The Wizard setup walks you through the most common configuration settings. We suggest you use this mode if it is the first time you are setting up your device.
Use Advanced mode if you need access to more advanced features.
Go to Wizard setup
Go to Advanced setup
Choose your language below
English
Deutsch
Français
Español
繁體中文
Italiano
簡体中文
Exit

2 Choose a language by clicking on the language's button. The screen will update. Click the **Next** button to proceed to the next screen.

Figure 15 Select a Language

3 Read the on-screen information and click **Next**.

Figure 16 Welcome to the Connection Wizard


Welcome to the ZyXEL Connection Wizard
The connection wizard will walk you through the most common configuration options. This wizard has been broken down into three steps, each of which may have multiple pages.
This wizard will take you through the following steps:
Step 1 : System Information Setup.
Step 2 : Wireless LAN Setup.
Step 3 : Internet Configuration Setup.
<Back
Next >
Exit

4.3 STEP 1: System Information

System Information contains administrative and system-related information.

4.3.1 System Name

System Name is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

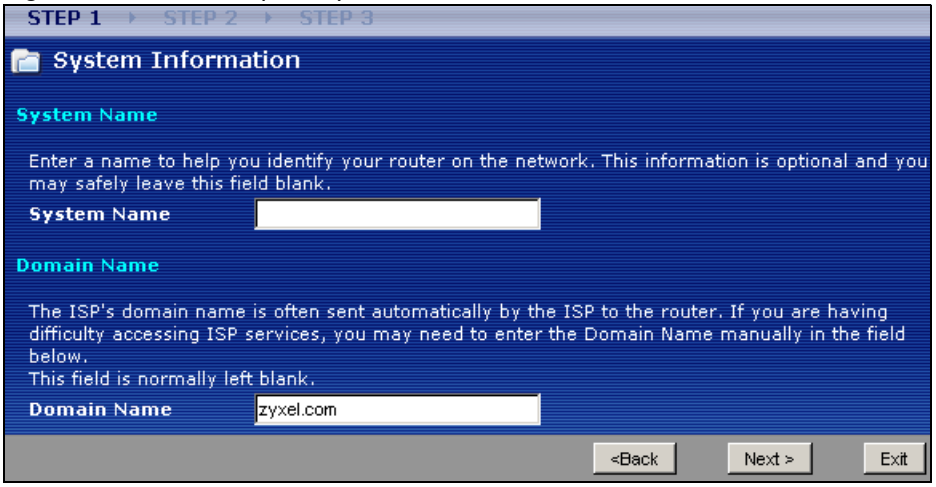
- In Windows 2000, click **Start** > **Settings** > **Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **System Name**.
- In Windows XP, click **Start** > **My Computer** > **View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the NBG4115 **System Name**.

4.3.2 Domain Name

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by DHCP from the ISP is used. While you must enter the host name (System Name) on each individual computer, the domain name can be assigned from the NBG4115 via DHCP.

Click **Next** to configure the NBG4115 for Internet access.

Figure 17 Wizard Step 1: System Information


STEP 1
STEP 2
STEP 3
System Information
System Name
Enter a name to help you identify your router on the network. This information is optional and you may safely leave this field blank.
System Name
Domain Name
The ISP's domain name is often sent automatically by the ISP to the router. If you are having difficulty accessing ISP services, you may need to enter the Domain Name manually in the field below.
This field is normally left blank.
Domain Name
zyxel.com
<Back
Next >
Exit

The following table describes the labels in this screen.

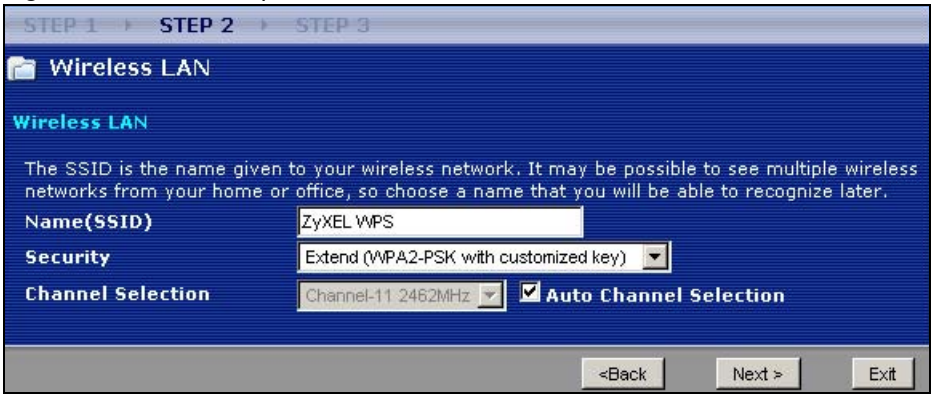
Table 13 Wizard Step 1: System Information

LABEL	DESCRIPTION
System Name	System Name is a unique name to identify the NBG4115 in an Ethernet network. Enter a descriptive name. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Type the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. The domain name entered by you is given priority over the ISP assigned domain name.
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.
Exit	Click **Exit** to close the wizard screen without saving.

4.4 STEP 2: Wireless LAN

Set up your wireless LAN using the following screen.

Figure 18 Wizard Step 2: Wireless LAN


STEP 1
STEP 2
STEP 3
Wireless LAN
Wireless LAN
The SSID is the name given to your wireless network. It may be possible to see multiple wireless networks from your home or office, so choose a name that you will be able to recognize later.
Name(SSID)
ZyXEL WPS
Security
Extend (WPA2-PSK with customized key)
Channel Selection
Channel-11 2462MHz
Auto Channel Selection
<Back
Next >
Exit

The following table describes the labels in this screen.

Table 14 Wizard Step 2: Wireless LAN

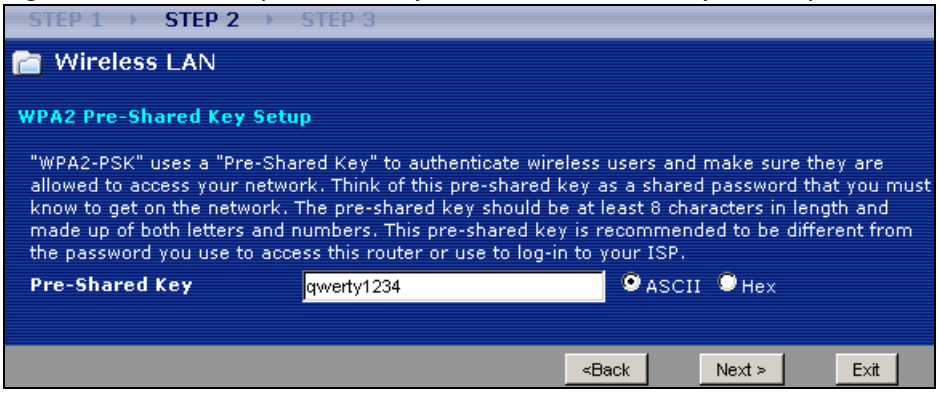
LABEL	DESCRIPTION
Name (SSID)	Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. If you change this field on the NBG4115, make sure all wireless stations use the same SSID in order to access the network.
Security	Select a **Security** level from the drop-down list box. Choose **Auto (WPA2-PSK)** to have the NBG4115 generate a pre-shared key automatically. After you click **Next** a screen pops up displaying the generated pre-shared key. Write down the key for use later when connecting other wireless devices to your network. Click **OK** to continue. Choose **None** to have no wireless LAN security configured. If you do not enable any wireless security on your NBG4115, your network is accessible to any wireless networking device that is within range. If you choose this option, skip directly to Section 4.5 on page 45. Choose **Extend** (**WPA-PSK** or **WPA2-PSK**) security to configure a Pre-Shared Key. Choose this option only if your wireless clients support WPA-PSK or WPA2-PSK respectively. If you choose this option, skip directly to Section 4.4.1 on page 44.
Channel Selection	The range of radio frequencies used by IEEE 802.11b/g/n wireless devices is called a channel. The device will automatically select the channel with the least interference.
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.
Exit	Click **Exit** to close the wizard screen without saving.

Note: The wireless stations and NBG4115 must use the same SSID, channel ID, WPA-PSK (if WPA-PSK is enabled) or WPA2-PSK (if WPA2-PSK is enabled) for wireless communication.

4.4.1 Extend (WPA-PSK or WPA2-PSK) Security

Choose **Extend (WPA-PSK)** or **Extend (WPA2-PSK)** security in the Wireless LAN setup screen to set up a **Pre-Shared Key**.

Figure 19 Wizard Step 2: Extend (WPA-PSK or WPA2-PSK) Security


STEP 1
STEP 2
STEP 3
Wireless LAN
WPA2 Pre-Shared Key Setup
"WPA2-PSK" uses a "Pre-Shared Key" to authenticate wireless users and make sure they are allowed to access your network. Think of this pre-shared key as a shared password that you must know to get on the network. The pre-shared key should be at least 8 characters in length and made up of both letters and numbers. This pre-shared key is recommended to be different from the password you use to access this router or use to log-in to your ISP.
Pre-Shared Key
qwerty1234
ASCII
Hex
<Back
Next >
Exit

The following table describes the labels in this screen.

Table 15 Wizard Step 2: Extend (WPA-PSK or WPA2-PSK) Security

LABEL	DESCRIPTION
Pre-Shared Key	Type from 8 to 63 case-sensitive **ASCII** or **HEX** characters. You can set up the most secure wireless connection by configuring WPA in the wireless LAN screens. You need to configure an authentication server to do this.
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.
Exit	Click **Exit** to close the wizard screen without saving.

4.5 STEP 3: Internet Configuration

The NBG4115 offers four Internet connection types. They are **Ethernet**, **PPP over Ethernet**, **PPTP** or **Mobile 3G**. The wizard attempts to detect which WAN connection type you are using. If the wizard does not detect a connection type, you must select one from the drop-down list box.

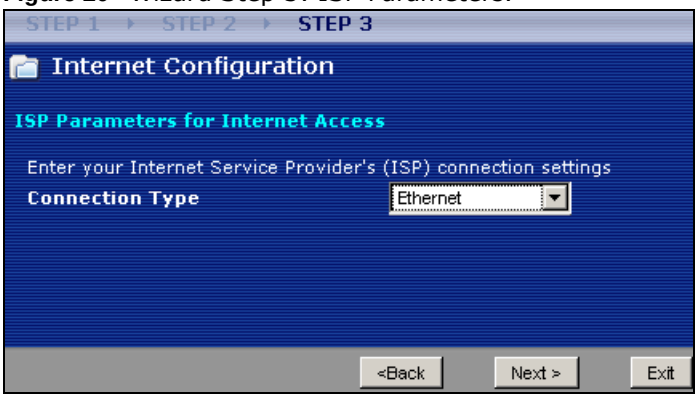
If you have an always-on connection, most likely you should use **Ethernet**. If your connection requires a user name and password to authenticate your connection, then choose either **PPPoE** or **PPTP**. Finally, if you are using a USB-based 3G device, select the **Mobile 3G** option.

Note: When you select Mobile 3G, then all WAN connections are made through this.

Check with your ISP to make sure you use the correct type.

This wizard screen varies according to the connection type that you select.

Figure 20 Wizard Step 3: ISP Parameters.



The following table describes the labels in this screen,

Table 16 Wizard Step 3: ISP Parameters

CONNECTION TYPE	DESCRIPTION
Ethernet	Select the **Ethernet** option when the WAN port is used as a regular Ethernet.
PPPoE	Select the **PPP over Ethernet** option for a dial-up connection. If your ISP gave you an IP address and/or subnet mask, then select **PPTP**.

Table 16 Wizard Step 3: ISP Parameters

CONNECTION TYPE	DESCRIPTION
PPTP	Select the **PPTP** option for a dial-up connection.
Mobile 3G	Select the **Mobile 3G** option for a USB 3G connection.

4.5.1 Ethernet Connection

Choose **Ethernet** when the WAN port is used as a regular Ethernet. Continue to Section 4.5.5 on page 50.

Figure 21 Wizard Step 3: Ethernet Connection

4.5.2 PPPoE Connection

Point-to-Point Protocol over Ethernet (PPPoE) functions as a dial-up connection. PPPoE is an IETF (Internet Engineering Task Force) standard specifying how a host personal computer interacts with a broadband modem (for example DSL, cable, wireless, etc.) to achieve access to high-speed data networks.

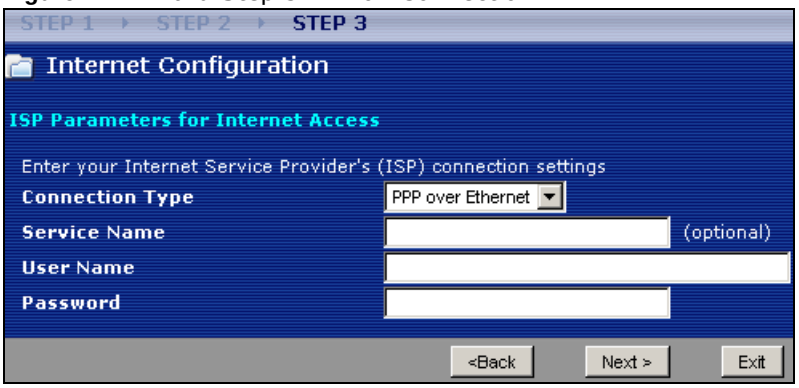
For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for instance, RADIUS).

One of the benefits of PPPoE is the ability to let end users access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for specific users.

Operationally, PPPoE saves significant effort for both the subscriber and the ISP/carrier, as it requires no specific configuration of the broadband modem at the subscriber's site.

By implementing PPPoE directly on the NBG4115 (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the NBG4115 does that part of the task. Furthermore, with NAT, all of the LAN's computers will have Internet access.

Figure 22 Wizard Step 3: PPPoE Connection



The following table describes the labels in this screen.

Table 17 Wizard Step 3: PPPoE Connection

LABEL	DESCRIPTION
ISP Parameter for Internet Access	
Connection Type	Select the **PPP over Ethernet** option for a dial-up connection.
Service Name	Type the name of your service provider.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.
Exit	Click **Exit** to close the wizard screen without saving.

4.5.3 PPTP Connection

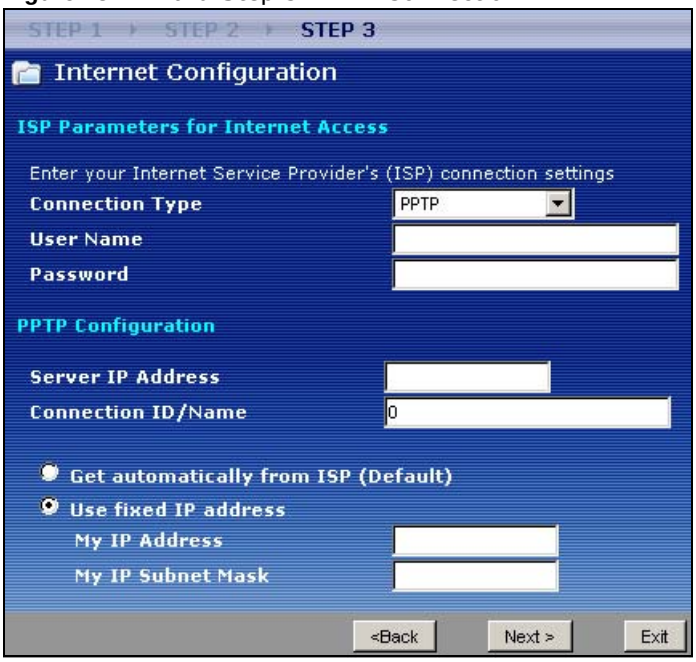
Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables transfers of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet.

Refer to the appendix for more information on PPTP.

Note: The NBG4115 supports one PPTP server connection at any given time.

Figure 23 Wizard Step 3: PPTP Connection



The following table describes the fields in this screen

Table 18 Wizard Step 3: PPTP Connection

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Connection Type	Select **PPTP** from the drop-down list box. To configure a PPTP client, you must configure the **User Name** and **Password** fields for a PPP connection and the PPTP parameters for a PPTP connection.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
PPTP Configuration	
Server IP Address	Type the IP address of the PPTP server.
Connection ID/ Name	Enter the connection ID or connection name in this field. It must follow the "c:id" and "n:name" format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your ISP.
Get automatically from ISP	Select this radio button if your ISP did not assign you a fixed IP address.
Use fixed IP address	Select this radio button, provided by your ISP to give the NBG4115 a fixed, unique IP address.
My IP Address	Type the (static) IP address assigned to you by your ISP.
My IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.
Exit	Click **Exit** to close the wizard screen without saving.

4.5.4 Mobile 3G

Mobile 3G is a set of international "third generation" standards for the sending and receiving of voice, video, and wireless data in a mobile environment. For the NBG4115, this type of wireless connection requires a connected 3G-compatible USB device (see the included Quick Start Guide for installation information), and a 3G account with your local ISP.

Note: When you use Mobile 3G, all WAN connections are made through it.

Figure 24 Wizard Step 3: Mobile 3G Connection

The following table describes the fields in this screen

Table 19 Wizard Step 3: Mobile 3G Connection

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Connection Type	Select **Mobile 3G** from the drop-down list box.
PIN Code	Enter the 4-digit 3G account PIN code given to you by your ISP.
APN Code	Enter the Access Point Name (APN) given to you by your ISP.
Dial Number	Enter the phone number that must be dialed in order to login to your 3G account from the NBG4115.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.
Exit	Click **Exit** to close the wizard screen without saving.

4.5.5 Your IP Address

The following wizard screen allows you to assign a fixed IP address or give the NBG4115 an automatically assigned IP address depending on your ISP or network administrator.

Figure 25 Wizard Step 3: Your IP Address

The following table describes the labels in this screen

Table 20 Wizard Step 3: Your IP Address

LABEL	DESCRIPTION
Get automatically from your ISP	Select this option if the ISP or your network administrator did not assign a static IP address to use for Internet access. This is the default selection. If you choose this option, skip directly to Section 4.5.10 on page 53.
Use fixed IP address provided by your ISP	Select this option if you were assigned a fixed IP address (and DNS server settings) to use for Internet access The fixed IP address should be in the same subnet as your broadband modem or router.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.
Exit	Click **Exit** to close the wizard screen without saving.

4.5.6 WAN IP Address Assignment

Every computer on the Internet must have a unique IP address. If your networks are isolated from the Internet, for instance, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks.

Table 21 Private IP Address Ranges

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

You can obtain your IP address from the IANA, from an ISP or have it assigned by a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Note: Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

4.5.7 IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your NBG4115, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your NBG4115 will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the NBG4115 unless you are instructed to do otherwise.

4.5.8 DNS Server Address Assignment

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.zyxel.com is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

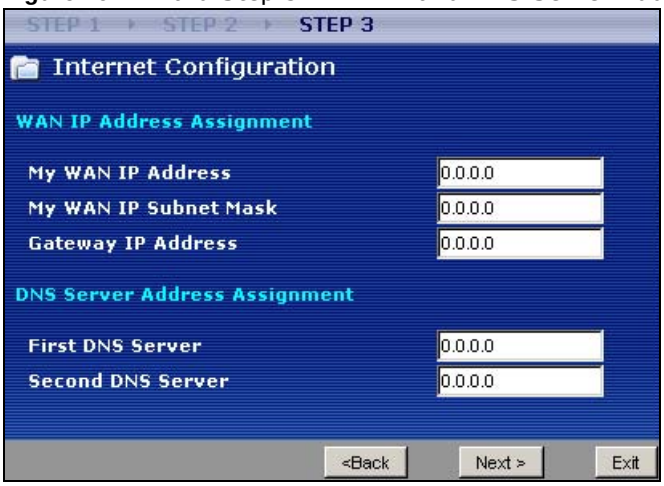
The NBG4115 can get the DNS server addresses in the following ways.

1. The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the **DNS Server** fields in the **Wizard** and/or **WAN > Internet Connection** screen.
2. If the ISP did not give you DNS server information, leave the **DNS Server** fields set to **0.0.0.0** in the **Wizard** screen and/or set to **From ISP** in the **WAN > Internet Connection** screen for the ISP to dynamically assign the DNS server IP addresses.

4.5.9 WAN IP and DNS Server Address Assignment

The following wizard screen allows you to assign a fixed WAN IP address and DNS server addresses.

Figure 26 Wizard Step 3: WAN IP and DNS Server Addresses



The following table describes the labels in this screen

Table 22 Wizard Step 3: WAN IP and DNS Server Addresses

LABEL	DESCRIPTION
WAN IP Address Assignment	
My WAN IP Address	Enter your WAN IP address in this field. The WAN IP address should be in the same subnet as your DSL/Cable modem or router.
My WAN IP Subnet Mask	Enter the IP subnet mask in this field.
Gateway IP Address	Enter the gateway IP address in this field.
System DNS Server Address Assignment (if applicable) DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The NBG4115 uses a system DNS server (in the order you specify here) to resolve domain names for DDNS and the time server.	
First DNS Server Second DNS Server	Enter the DNS server's IP address in the fields provided. If you do not configure a system DNS server, you must use IP addresses when configuring DDNS and the time server.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.
Exit	Click **Exit** to close the wizard screen without saving.

4.5.10 WAN MAC Address

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

Table 23 Example of Network Properties for LAN Servers with Fixed IP Addresses

Choose an IP address	192.168.1.2-192.168.1.32; 192.168.1.65-192.168.1.254.
Subnet mask	255.255.255.0
Gateway (or default route)	192.168.1.1(NBG4115 LAN IP)

This screen allows users to configure the WAN port's MAC address by either using the NBG4115's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address. Once it is successfully configured, the address will be copied to configuration file. It is advisable to clone the MAC address from a computer on your LAN even if your ISP does not presently require MAC address authentication.

Figure 27 Wizard Step 3: WAN MAC Address

STEP 1
STEP 2
STEP 3
Internet Configuration
WAN MAC Address
Users configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Select Factory Default to use the factory assigned default MAC address. Alternatively, select Spoof this Computer's MAC address - IP Address and enter the IP address of the computer on the LAN whose MAC address you are cloning.
Factory default
Clone the computer's MAC address
IP Address
0.0.0.0
Set WAN MAC Address
00:00:00:00:00:00
<Back
Next >
Exit

The following table describes the fields in this screen.

Table 24 Wizard Step 3: WAN MAC Address

LABEL	DESCRIPTION
Factory Default	Select **Factory Default** to use the factory assigned default MAC address.
Clone the computer's MAC address	Select this option and enter the IP address of the computer on the LAN whose MAC you are cloning. It is advisable to clone the MAC address from a computer on your LAN even if your ISP does not presently require MAC address authentication.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.
Exit	Click **Exit** to close the wizard screen without saving.

4.6 Connection Wizard Complete

Click **Finish** to complete the wizard setup.

Figure 28 Connection Wizard Complete

Congratulation!
The Connection Wizard configuration is complete.
Please press "Finish" button to complete Connection Wizard.
Check our exciting range of ZyXEL products at www.zyxel.com
Having Internet access problems?
1. Verify your settings in this wizard.
2. If your wizard entries are correct, but still cannot access the Internet, then check that your ISP account is active and that the settings you entered in the wizard are correct.
3. If you still have problems, please contact customer support.
Finish

You have successfully set up your NBG4115 to operate on your network and access the Internet.

5

AP Mode

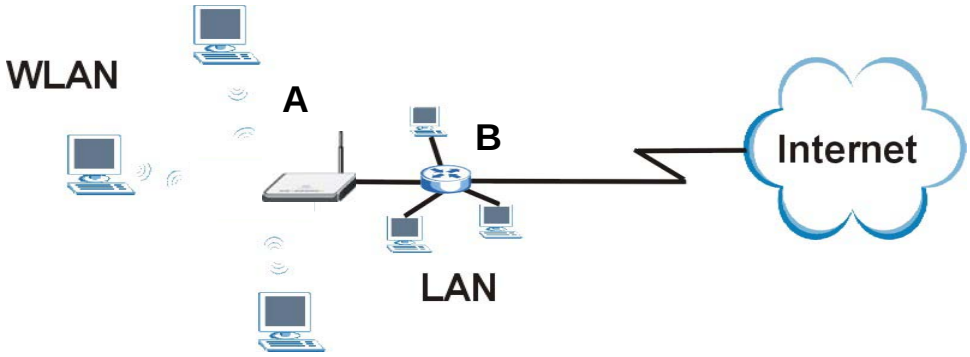
5.1 Overview

This chapter discusses how to configure settings while your NBG4115 is set to **AP Mode**. Many screens that are available in **Router Mode** are not available in **AP Mode**.

Note: See Chapter 6 on page 61 for an example of setting up a wireless network in AP mode.

Use your NBG4115 as an AP if you already have a router or gateway on your network. In this mode your device bridges a wired network (LAN) and wireless LAN (WLAN) in the same subnet. See the figure below for an example.

Figure 29 Wireless Internet Access in AP Mode

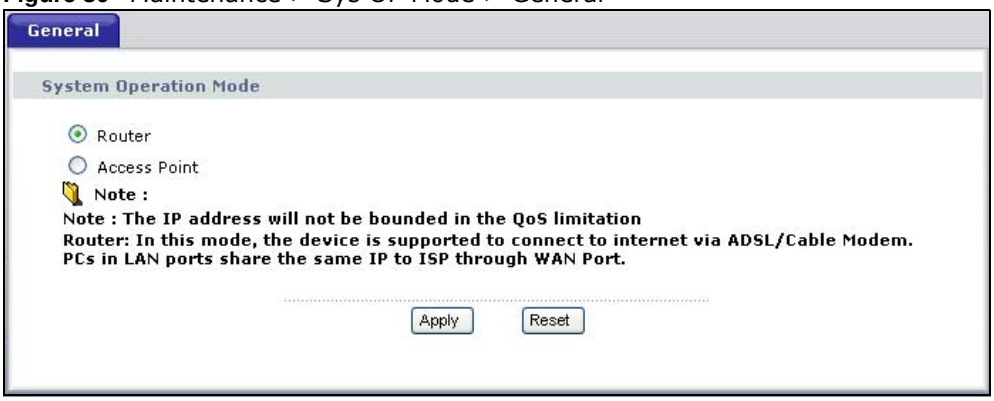


5.2 Setting your NBG4115 to AP Mode

1 Log into the Web Configurator if you haven't already. See the Quick start Guide for instructions on how to do this.

2 To set your NBG4115 to **AP Mode**, go to **Maintenance > Sys OP Mode > General** and select **Access Point.**

Figure 30 Maintenance > Sys OP Mode > General


General
System Operation Mode
Router
Access Point
Note :
Note : The IP address will not be bounded in the QoS limitation
Router: In this mode, the device is supported to connect to internet via ADSL/Cable Modem.
PCs in LAN ports share the same IP to ISP through WAN Port.
Apply
Reset

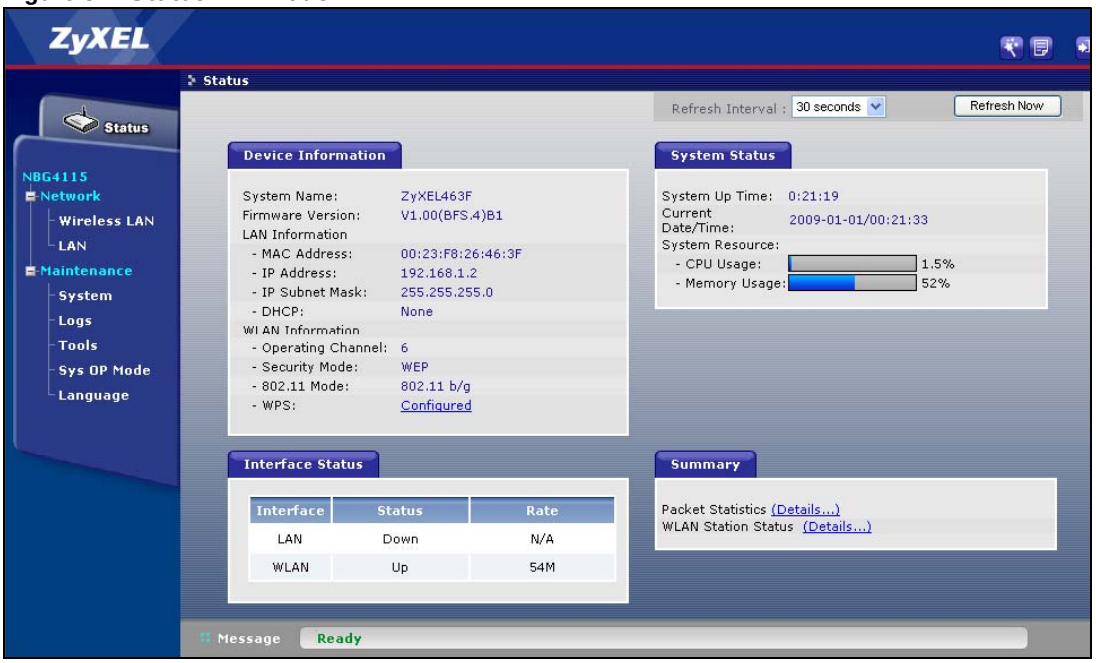
3 A pop-up appears providing information on this mode. Click **OK** in the pop-up message window. (See Section 24.2 on page 182 for more information on the pop-up.) Click **Apply**. Your NBG4115 is now in **AP Mode**.

Note: You have to log in to the Web Configurator again when you change modes.

5.3 The Status Screen in AP Mode

Click on **Status**. The screen below shows the status screen in **AP Mode**.

Figure 31 Status: AP Mode



The following table describes the labels shown in the **Status** screen.

Table 25 Web Configurator Status Screen

LABEL	DESCRIPTION
Device Information	
System Name	This is the **System Name** you enter in the **Maintenance** > **System** > **General** screen. It is for identification purposes.
Firmware Version	This is the firmware version and the date created.
LAN Information	
- MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
- IP Address	This shows the LAN port's IP address.
- IP Subnet Mask	This shows the LAN port's subnet mask.
- DHCP	This shows the LAN port's DHCP role - **None**.
WLAN Information	
- MAC Address	This shows the wireless adapter MAC Address of your device.
- Status	This shows the current status of the Wireless LAN - **On**, **Off or Off by scheduler**.
- Name (SSID)	This shows a descriptive name used to identify the NBG4115 in the wireless LAN.
- Channel	This shows the channel number which you select manually.
- Operating Channel	This shows the channel number which the NBG4115 is currently using over the wireless LAN.
- Security Mode	This shows the level of wireless security the NBG4115 is using.
- 802.11 Mode	This shows the IEEE 802.11 standard that the NBG4115 supports. Wireless clients must support the same standard in order to be able to connect to the NBG4115
- WPS	This shows the WPS (WiFi Protected Setup) Status. Click the status to display **Network** > **Wireless LAN** > **WPS** screen.
System Status	
System Up Time	This is the total time the NBG4115 has been on.
Current Date/Time	This field displays your NBG4115's present date and time.
System Resource	
- CPU Usage	This displays what percentage of the NBG4115's processing ability is currently used. When this percentage is close to 100%, the NBG4115 is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications.
- Memory Usage	This shows what percentage of the heap memory the NBG4115 is using.
Interface Status	
Interface	This displays the NBG4115 port types. The port types are: **LAN** and **WLAN**.
Status	For the LAN port, this field displays **Down** (line is down) or **Up** (line is up or connected). For the WLAN, it displays **Up** when the WLAN is enabled or **Down** when the WLAN is disabled.
Rate	For the LAN ports, this displays the port speed and duplex setting or **N/A** when the line is disconnected. For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and **N/A** when the WLAN is disabled.
Summary	

Table 25 Web Configurator Status Screen (continued)

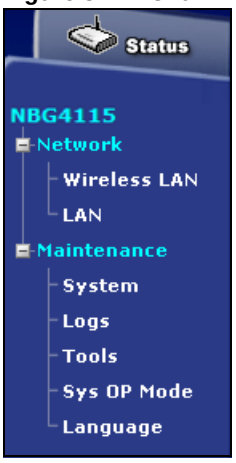
LABEL	DESCRIPTION
Packet Statistics	Use this screen to view port status and packet specific statistics.
WLAN Station Status	Use this screen to view the wireless stations that are currently associated to the NBG4115.

5.3.1 Navigation Panel

Use the menu in the navigation panel to configure NBG4115 features in **AP Mode**.

The following screen and table show the features you can configure in **AP Mode**.

Figure 32 Menu: AP Mode



The following table describes the sub-menus.

Table 26 Screens Summary

LINK	TAB	FUNCTION
Status		This screen shows the NBG4115's general device, system and interface status information. Use this screen to access the wizard, and summary statistics tables.
Network		
Wireless LAN	General	Use this screen to configure wireless LAN.
	MAC Filter	Use the MAC filter screen to configure the NBG4115 to block access to devices or block the devices from accessing the NBG4115.
	Advanced	This screen allows you to configure advanced wireless settings.
	QoS	Use this screen to configure Wi-Fi Multimedia Quality of Service (WMM QoS). WMM QoS allows you to prioritize wireless traffic according to the delivery requirements of individual services.
	WPS	Use this screen to configure WPS.
	WPS Station	Use this screen to add a wireless station using WPS.
	Scheduling	Use this screen to schedule the times the Wireless LAN is enabled.
LAN	IP	Use this screen to configure LAN IP address and subnet mask or to get the LAN IP address from a DHCP server.
Maintenance		

Table 26 Screens Summary

LINK	TAB	FUNCTION
System	General	Use this screen to view and change administrative settings such as system and domain names, password and inactivity timer.
	Time Setting	Use this screen to change your NBG4115's time and date.
Logs	View Log	Use this screen to view the logs for the categories that you selected.
Tools	Firmware	Use this screen to upload firmware to your NBG4115.
	Configuration	Use this screen to backup and restore the configuration or reset the factory defaults to your NBG4115.
	Restart	This screen allows you to reboot the NBG4115 without turning the power off.
Sys OP Mode	General	This screen allows you to select whether your device acts as a Router or a Access Point.
Language		This screen allows you to select the language you prefer.

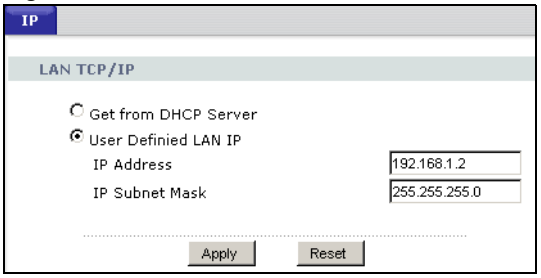
5.4 LAN Settings

Use this section to configure your LAN settings while in **AP Mode**.

Click **Network > LAN** to see the screen below.

Note: If you change the IP address of the NBG4115 in the screen below, you will need to log into the NBG4115 again using the new IP address.

Figure 33 Network > LAN > IP



The table below describes the labels in the screen.

Table 27 Network > LAN > IP

LABEL	DESCRIPTION
Get from DHCP Server	Select this to let the DHCP server in the gateway assign the NBG4115 IP address.
User Defined LAN IP	Select this to give the NBG4115 a static IP address.
IP Address	Type the IP address in dotted decimal notatiion. The default setting is 192.168.1.2. If you change the IP address you will have to log in again with the new IP address.

LABEL	DESCRIPTION
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your NBG4115 will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the NBG4115.
Apply	Click **Apply** to save your changes to the NBG4115.
Reset	Click **Reset** to reload the previous configuration for this screen.

5.5 WLAN and Maintenance Settings

The configuration of wireless and maintenance settings in **AP Mode** is the same as for **Router Mode**.

- See Wireless LAN (77) for information on the configuring your wireless network.
- See System (169), Logs (174), Tools (176), Sys OP Mode (181) and Language (184) for information on the configuring your Maintenance settings.

5.6 Logging in while in AP Mode

1. Connect your computer to the LAN port of the NBG4115.
2. The default IP address of the NBG4115 is "192.168.1.2". In this case, your computer must have an IP address in the range between "192.168.1.3" and "192.168.1.254".
3. Click **Start > Run** on your computer in Windows.
4. Type "cmd" in the dialog box.
5. Type "ipconfig" to show your computer's IP address. If your computer's IP address is not in the correct range then see Appendix C on page 215 for information on changing your computer's IP address.
6. After you've set your computer's IP address, open a web browser such as Internet Explorer and type "192.168.1.2" as the web address in your web browser.

   See Chapter 6 on page 61 for a tutorial on setting up a network with an AP.

6 Tutorials

6.1 Overview

This chapter provides tutorials for setting up your NBG4115.

6.2 Set Up a 3G Connection

This section shows you how to make a 3G connection with your NBG4115. There are two ways to set up your 3G options.

1 Use the **Wizard**, which was introduced in the Quick Start Guide. The wizard is good for getting up and running in as little time as possible. It allows you to configure the minimum number of options required to get connected.

2 Use the Web Configurator's **Network** options. This is handy because it gives you access to other options not available in the Wizard, allowing you to have more control over your device.

This tutorial shows you how to do the second one.

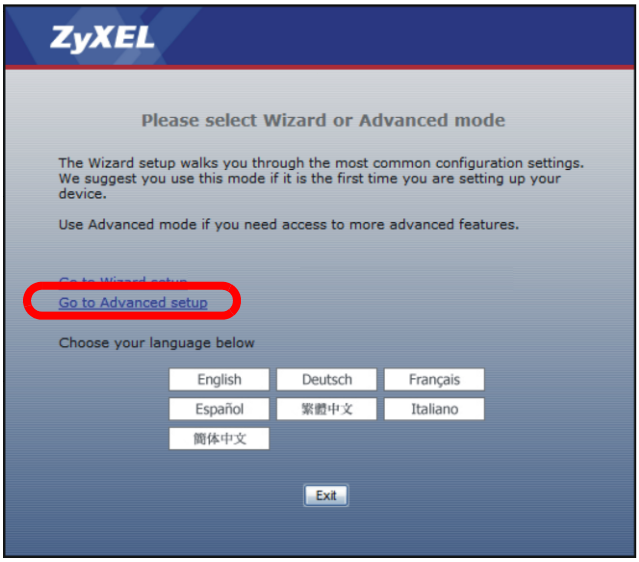
You will need the following information, which should be provided by your ISP:

FIELD	DESCRIPTION	EXAMPLE
PIN Code	This is the 4-digit Personal Identification Number (PIN) for your 3G device's SIM card.	1234
APN Code	This is the Access Point Name (APN) of the 3G network to which you intend to connect.	mobile.p3.cz.co gprsinternet
Dial Number	This is the number used to instruct your 3G device to make its data connection to the 3G network.	*99# *99***3#
User Name	This is your account user name.	dcmchale 0b1ken@kashiik.org
Password	This is your account user name's password.	*****

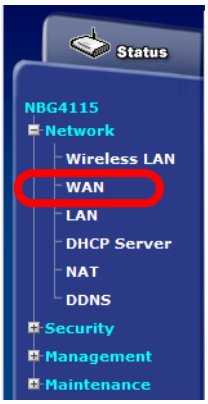
To set up a 3G connection:

1 Connect to the Web Configurator, as described in the Quick Start Guide.

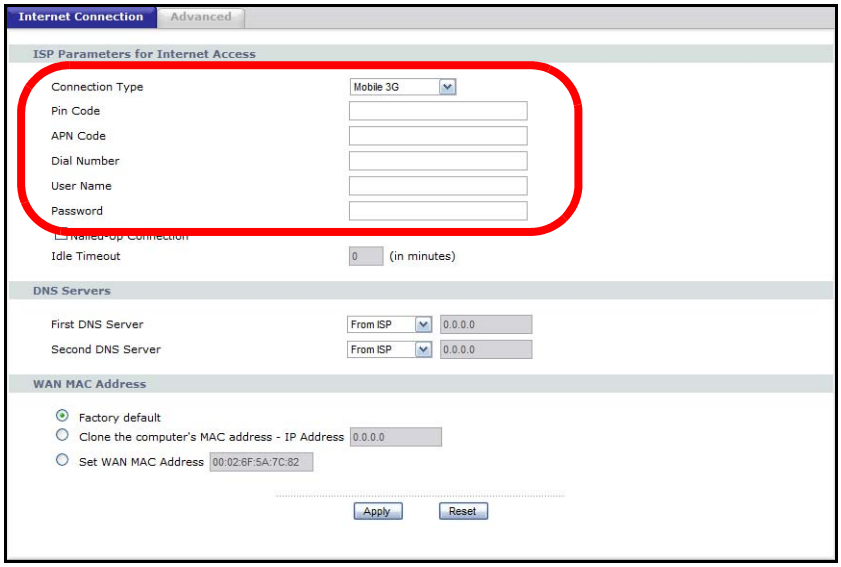
2 When presented with the option to choose either **Wizard** or **Advanced**, click **Go to Advanced setup**.


ZyXEL
Please select Wizard or Advanced mode
The Wizard setup walks you through the most common configuration settings. We suggest you use this mode if it is the first time you are setting up your device.
Use Advanced mode if you need access to more advanced features.
Go to Advanced setup
Choose your language below
English
Deutsch
Français
Español
繁體中文
Italiano
简体中文
Exit

3 Expand the **Network** submenu on the navigation pane, then click **WAN**.



4 From the **Connection Type** menu, select **Mobile 3G** then configure your 3G settings when the screen updates itself.f



5 Click **Apply** to save your changes, then exit the Web Configurator.

Note: Once you set up and enable a 3G device, all incoming and outgoing network connections are made through it and not the WAN port on your NBG4115.

6.3 Set Up the NBG4115 for Gaming

Gaming is a very popular online activity, and one that can be extremely bandwidth sensitive. Some video games may have higher performance expectations than other types of software. As such, they tend to require more finely tuned Quality of Service (QoS) prioritization. If the data packets from a game are assigned a lower priority by the NBG4115, then they may take longer to reach their destination; but if they are given a higher priority, then they should arrive at their destination marginally faster. This is because Internet servers that rely on QoS to sort packets that are in transit generally pass higher priority packets on first, while lower priority packets are held back slightly longer.

When this happens on a single server with a single data packet, your gameplay is not affected. When it happens over 15 servers from beginning to end with thousands of bytes of data, then the build up of low-priority latency can become significant. For Massively Multiplayer Online (MMOs) and First Person Shooters (FPS) (which account for 3-4% of all Internet-related traffic) a latency difference of even 200 milliseconds is enough to ruin the gaming experience.

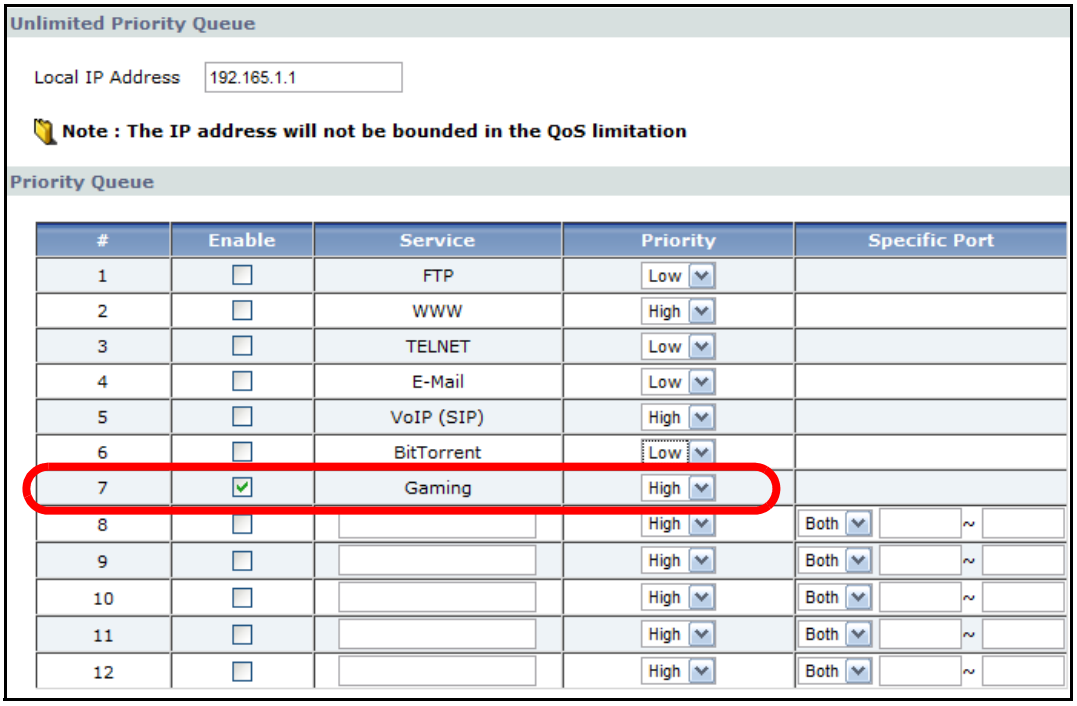
Bandwidth management allows you to set up custom parameters on the NBG4115 so that whenever you play a game, the QoS is automatically upgraded to the highest priority in order to ensure your game data packets are plucked first from the pool of incoming information and sent on ahead of lower priority packets.

This tutorial shows you how to set up your NBG4115 for gaming.

1 In the Web Configurator, expand the navigation pane's **Management** category and then select **Bandwidth MGMT**

2 Select the **Advanced** tab.

3 Enable the **Gaming** check box and set its **Priority** to High.



The following gaming ports are preconfigured on your NBG4115 and are enabled when you select the 'gaming' **Service** in the **Management** > **Bandwidth MGMT > Advanced** screen:

Table 28 Preconfigured Gaming Ports

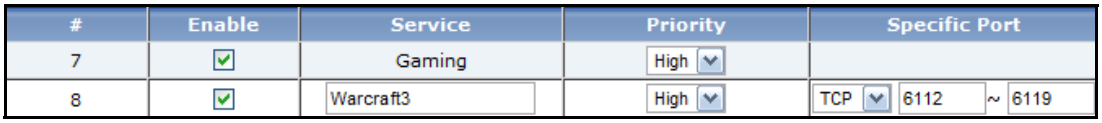
APPLICATION	TCP PORTS	UDP PORTS
XBox 360	3074, 3390, 3932, 5555	1900, 3776, 7777, 88, 3074
Playstation	80, 443, 5223, 5223	3478, 3479, 3658, 4658

Table 28 Preconfigured Gaming Ports

APPLICATION	TCP PORTS	UDP PORTS
Battlenet	40, 6112, 4000, 6113- 6119, 112	
MSN Game Zone	6667, 28800-29000	6667, 28800-29000

Note: If you need to customize specific ports, go to the next step. Otherwise, skip ahead to step 5.

4 To create a custom QoS setting for a specific game, enter the following information in the first available custom Priority Queue line:



Service: This is the name by which your custom service is labled. It can be anything with the limitation that it cannot be longer than 10 characters.

Priority: Set this to **High**.

Specific Port: From the list, select the communication protocol your game uses. In this example, our game uses TCP/IP so we choose **TCP**. If you are not sure, then select **Both**. Enter the starting port in the first port range box, then enter then last port in the second port range box. For our game, we used 6112 to 6119.

5 Click **Apply** to save your changes, then exit the Web Configurator.

6.4 Set Up a Wireless Network with WPS

This section gives you an example of how to set up wireless network using WPS. This example uses the NBG4115 as the AP and NWD210N as the wireless client which connects to a notebook.

Note: The wireless client must be a WPS-aware device (for example, a WPS USB adapter or PCI card).

There are two WPS methods for creating a secure connection. This tutorial shows you how to do both.

- **Push Button Configuration (PBC)** - create a secure wireless network simply by pressing a button. See Section 6.4.1 on page 66.This is the easier method.
- **PIN Configuration** - create a secure wireless network simply by entering a wireless client's PIN (Personal Identification Number) in the NBG4115's interface. See Section 6.4.2 on page 67. This is the more secure method, since one device can authenticate the other.

6.4.1 Push Button Configuration (PBC)

1. Make sure that your NBG4115 is turned on and that it is within range of your computer.
2. Make sure that you have installed the wireless client (this example uses the NWD210N) driver and utility in your notebook.
3. In the wireless client utility, find the WPS settings. Enable WPS and press the WPS button (**Start** or **WPS** button)
4. Log into NBG4115's Web Configurator and press the **Push Button** button in the **Network** > **Wireless Client** > **WPS Station** screen.

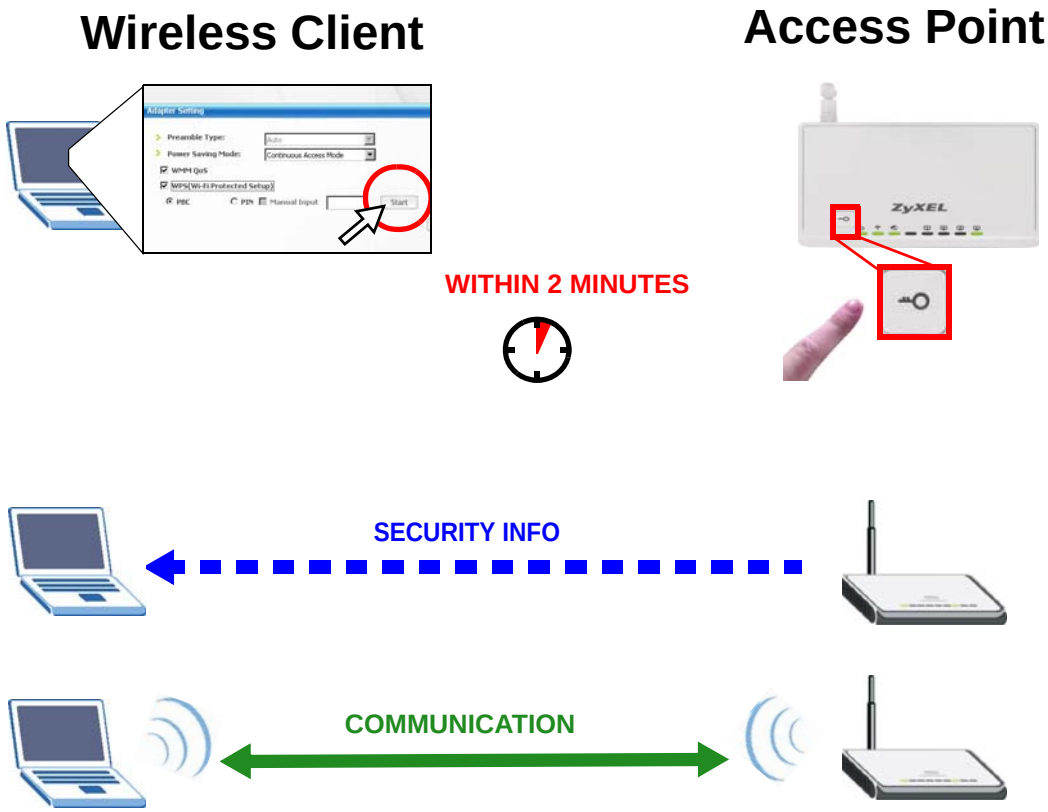
   Note: Your NBG4115 has a WPS button located on its panel, as well as a WPS button in its configuration utility. Both buttons have exactly the same function; you can use one or the other.

   Note: It doesn't matter which button is pressed first. You must press the second button within two minutes of pressing the first one.

   The NBG4115 sends the proper configuration settings to the wireless client. This may take up to two minutes. Then the wireless client is able to communicate with the NBG4115 securely.

The following figure shows you an example to set up wireless network and security by pressing a button on both NBG4115 and wireless client (the NWD210N in this example).

Figure 34 Example WPS Process: PBC Method



6.4.2 PIN Configuration

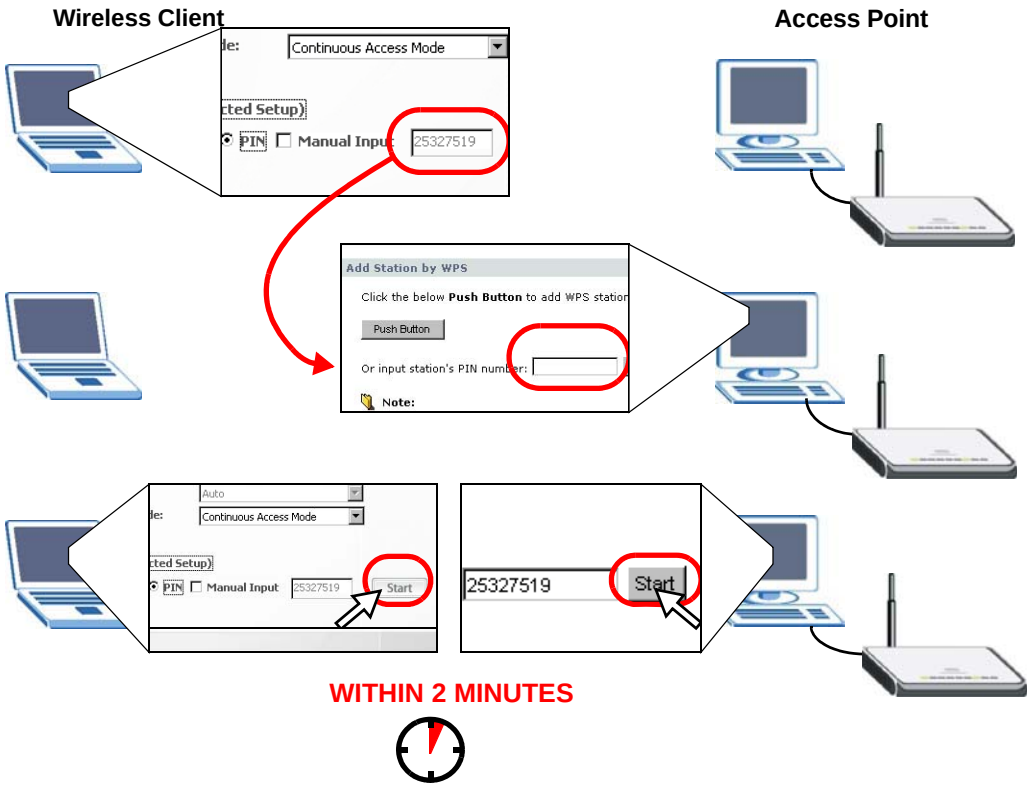
When you use the PIN configuration method, you need to use both NBG4115's configuration interface and the client's utilities.

1. Launch your wireless client's configuration utility. Go to the WPS settings and select the PIN method to get a PIN number.
2. Enter the PIN number to the **PIN** field in the **Network** > **Wireless LAN** > **WPS Station** screen on the NBG4115.
3. Click **Start** buttons (or button next to the PIN field) on both the wireless client utility screen and the NBG4115's **WPS Station** screen within two minutes.

   The NBG4115 authenticates the wireless client and sends the proper configuration settings to the wireless client. This may take up to two minutes. Then the wireless client is able to communicate with the NBG4115 securely.

The following figure shows you the example to set up wireless network and security on NBG4115 and wireless client (ex. NWD210N in this example) by using PIN method.

Figure 35 Example WPS Process: PIN Method



6.5 Configure Wireless Security without WPS

This example shows you how to configure wireless security settings with the following parameters on your NBG4115.

SSID	SSID_Example3
Channel	6
Security	WPA-PSK (Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey)

Follow the steps below to configure the wireless settings on your NBG4115.

The instructions require that your hardware is connected (see the Quick Start Guide) and you are logged into the Web Configurator through your LAN connection (see Section 3.2 on page 29).

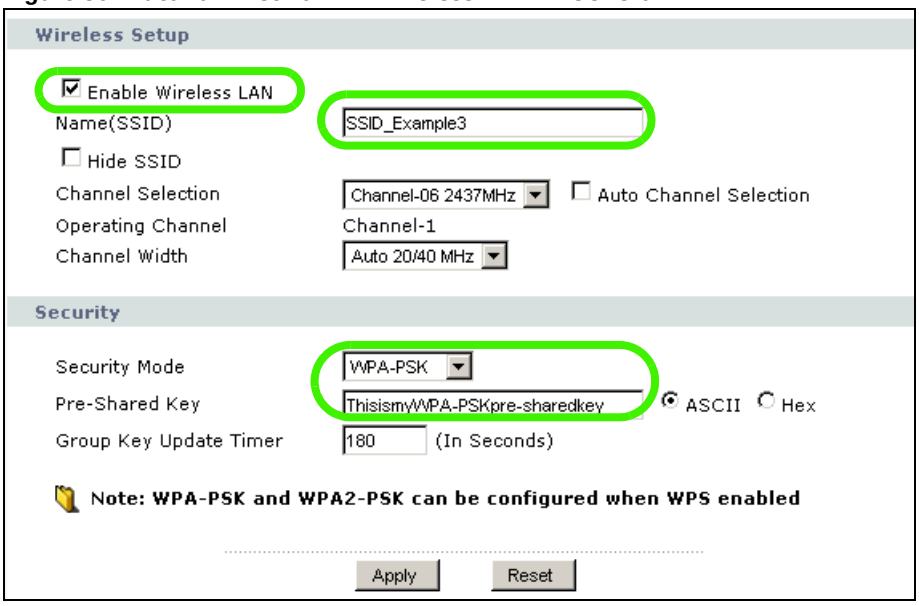
1 Open the **Wireless LAN > General** screen in the AP's Web Configurator.

2 Make sure the **Enable Wireless LAN** check box is selected.

3 Enter **SSID_Example3** as the SSID and select a channel.

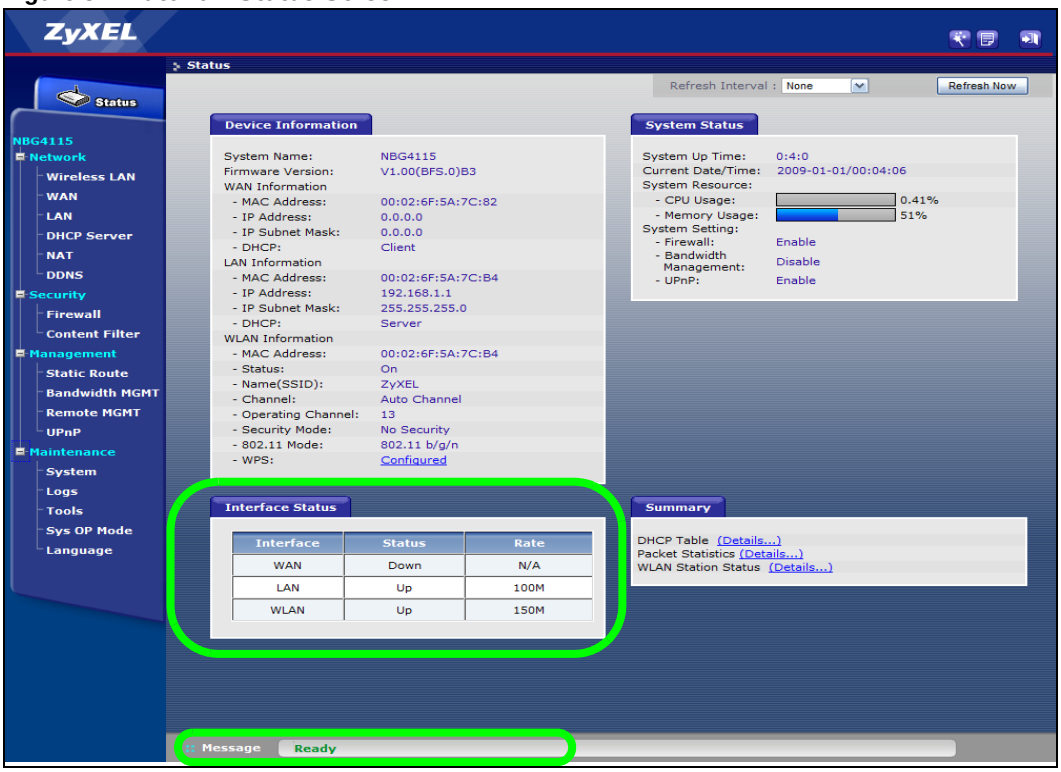
4 Set security mode to **WPA-PSK** and enter **ThisismyWPA-PSKpre-sharedkey** in the **Pre-Shared Key** field. Click **Apply**.

Figure 36 Tutorial: Network > Wireless LAN > General



5 Open the **Status** screen. Verify your wireless and wireless security settings under **Device Information** and check if the WLAN connection is up under **Interface Status**.

Figure 37 Tutorial: Status Screen



6.5.1 Configure Your Notebook

Note: We use the ZyXEL M-302 wireless adapter utility screens as an example for the wireless client. The screens may vary for different models.

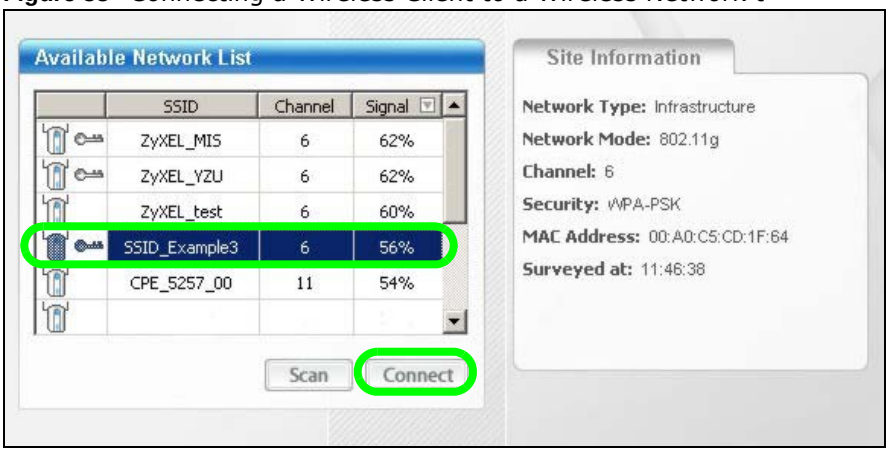
1 The NBG4115 supports IEEE 802.11b, IEEE 802.11g and IEEE 802.11n wireless clients. Make sure that your notebook or computer's wireless adapter supports one of these standards.

2 Wireless adapters come with software sometimes called a "utility" that you install on your computer. See your wireless adapter's User's Guide for information on how to do that.

3 After you've installed the utility, open it. If you cannot see your utility's icon on your screen, go to **Start > Programs** and click on your utility in the list of programs that appears. The utility displays a list of APs within range, as shown in the example screen below.

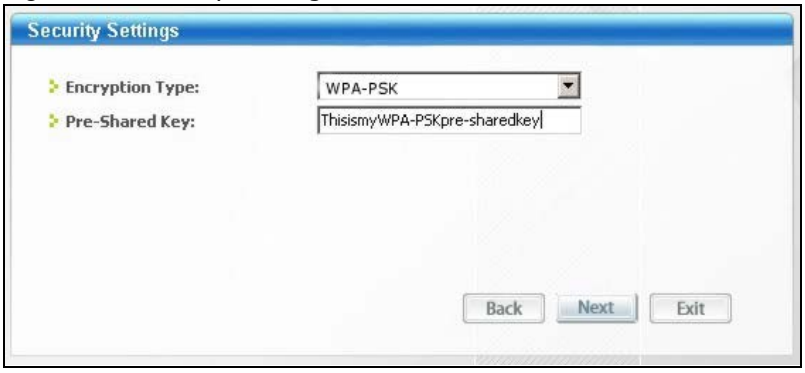
4 Select SSID_Example3 and click **Connect**.

Figure 38 Connecting a Wireless Client to a Wireless Network t



5 Select WPA-PSK and type the security key in the following screen. Click **Next**.

Figure 39 Security Settings

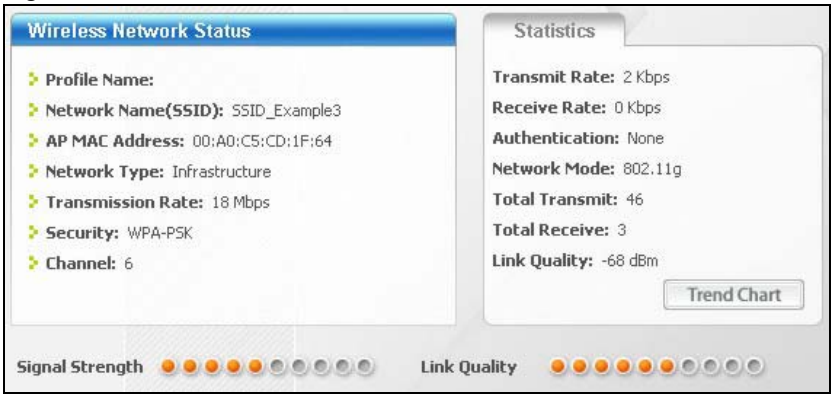


6 The **Confirm Save** window appears. Check your settings and click **Save** to continue.

Figure 40 Confirm Save

7 Check the status of your wireless connection in the screen below. If your wireless connection is weak or you have no connection, see the Troubleshooting section of this User's Guide.

Figure 41 Link Status



If your connection is successful, open your Internet browser and enter http://www.zyxel.com or the URL of any other web site in the address bar. If you are able to access the web site, your wireless connection is successfully configured.

6.6 Bandwidth Management

This section shows you how to configure the bandwidth management feature on the NBG4115 to limit the bandwidth for specific kinds of outgoing traffic. ZyXEL's bandwidth management feature allows you to specify bandwidth management rules based on an application or subnet.

Use the **Management > Bandwidth MGMT > Advanced** screen to configure bandwidth management for your network.

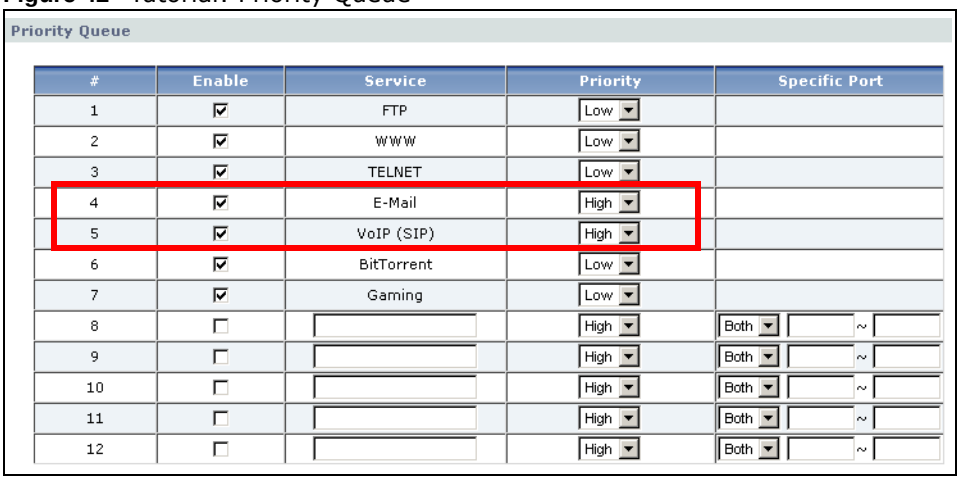
6.6.1 Bandwidth Management by Application

For this example, your company's customer support department wants to prioritize VoIP, e-mail and MSN Messenger services.

In the **Priority Queue** table, VoIP and e-mail services are already pre-defined. However, you still need to add MSN Messenger in the list (refer to Section 6.6.2 on page 72).

In the following screen, you set the priorities for VoIP and e-mail.

Figure 42 Tutorial: Priority Queue



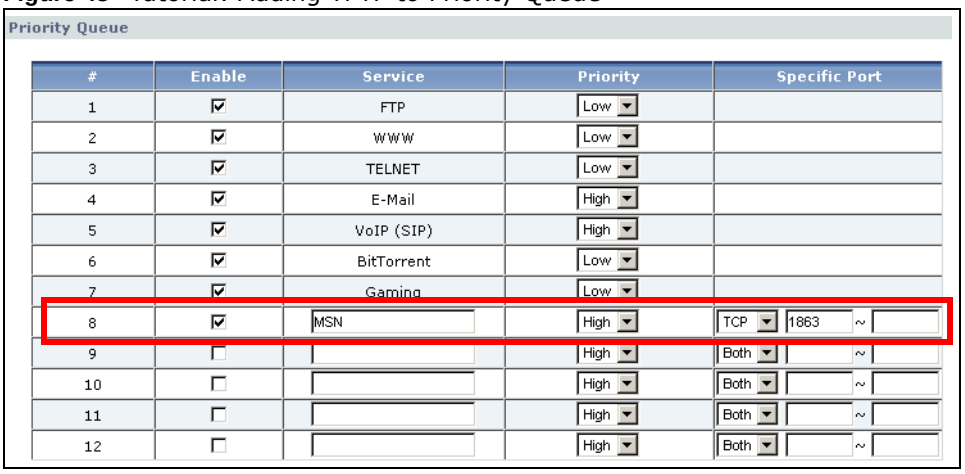
Click **Enable** for the VoIP (SIP) service and set priority to **High**. Do the same for E-mail. For the rest of the applications, click **Enable** if you need these services and set the priority to **Low**.

Note: You can also leave the **Enable** field blank for the rest of the applications. In doing so, the NBG4115 does not apply bandwidth management to these services.

6.6.2 Custom Bandwidth Management

Aside from the VOIP and e-mail services, you need to set the priority for MSN Messenger. To do this, add the service in the **Priority Queue** table of the **Management > Bandwidth MGMT > Advanced** screen.

Figure 43 Tutorial: Adding TFTP to Priority Queue



To add the MSN Messenger service in the **Priority Queue**:

1 Click **Enable** in one of the fields for additional services.

2 Add **MSN** as the service name.

3 Set the priority for this to **High**.

4 For the port, choose **TCP** from the drop-down menu and enter **1863** in the **Specific Port** field.

Your priority table should now have the VoIP, e-mail and MSN Messenger services priorities set to **High**.

6.6.3 Bandwidth Management by IP or IP Range

For this example, your company's 20th anniversary is coming up. You want to use the multimedia room's Internet connection to upload some videos to the website. You also use this room for video conferences, radio broadcasts, live video streaming, and so on throughout the day. While these media-heavy activities are going on, you still want to keep uploading the videos in the background. As such, you want to dedicate the minimum amount of bandwidth for this traffic.

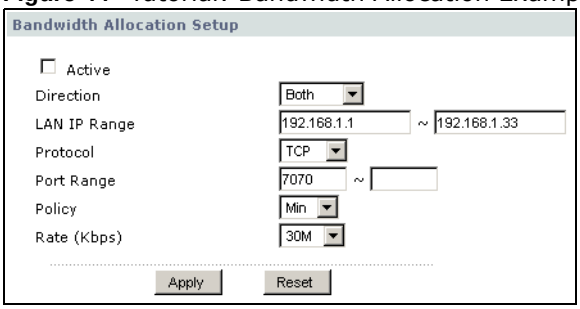
You know the following:

- Multimedia room's LAN IP range: 192.168.1.1 to 192.168.1.34
- IP Address of the computer uploading through FTP: 192.168.1.34
- Services you want to configure:

REAL AUDIO	TCP 7070
RTSP	TCP or UDP 554
VDO LIVE	TCP 7000
FTP	TCP 20 ~ 21

Click the **Edit** icon in **Management > Bandwidth MGMT** > **Advanced** to open the following screen. The following screen appears.

Figure 44 Tutorial: Bandwidth Allocation Example



Enter the following values for each service you want to add. For this tutorial, you need to add each of the following service (see table below) and click **Apply**.

Table 29

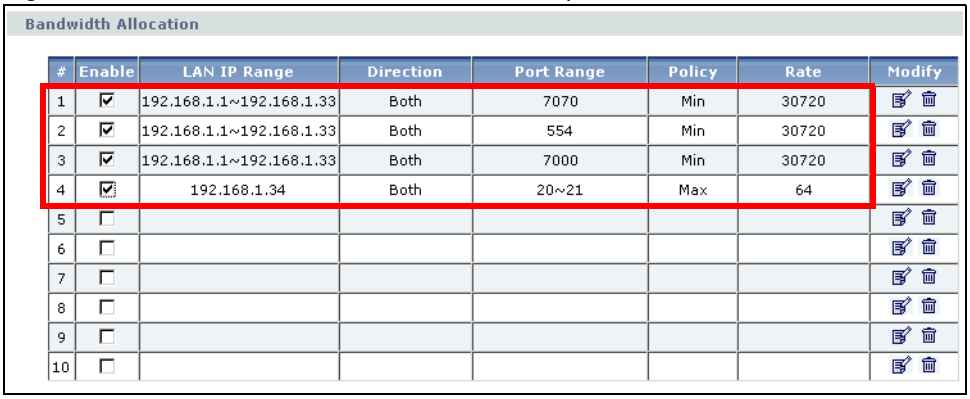
FIELDS	SERVICES			
	REAL AUDIO	**RTSP**	**VDO LIVE**	**FTP**
Active	Check this to turn on this bandwidth management rule.			
Direction	Select **Both** applies bandwidth management to traffic that the NBG4115 forwards to both the LAN and the WAN.			Select **To WAN**

Table 29

FIELDS	SERVICES			
	REAL AUDIO	**RTSP**	**VDO LIVE**	**FTP**
LAN IP Range	Enter **192.168.1.1 ~ 192.168.1.33**.			Enter **192.168.1.34**
Protocol	**TCP**	**TCP** or **UDP**	**TCP**	**TCP**
Port Range	**7070**	**554**	**7000**	**20 ~ 21**
Policy	**Min**			**Max**
Rate	Select **30M** as the minimum bandwidth allowed.			Select **64K**
Apply	Click this to add the rule to the **Bandwidth Allocation** table.			

After adding these services, go to **Management > Bandwidth MGMT** > **Advanced** and check if you have the correct values.

Figure 45 Tutorial: Bandwidth Allocation Example



Note: The **Policy** column displays either **Max** (maximum) or **Min** (minimum). This is directly directed to the value in the **Rate** column. For example, you selected **Min** and entered **30M** as the rate for the VoIP service. The NBG4115 allocates at least 30 megabytes for the VoIP service.

Refer to Appendix E on page 257 for a list of common services that you can add in the **Bandwidth Mgnt** screen.

PART II
Technical Reference

7

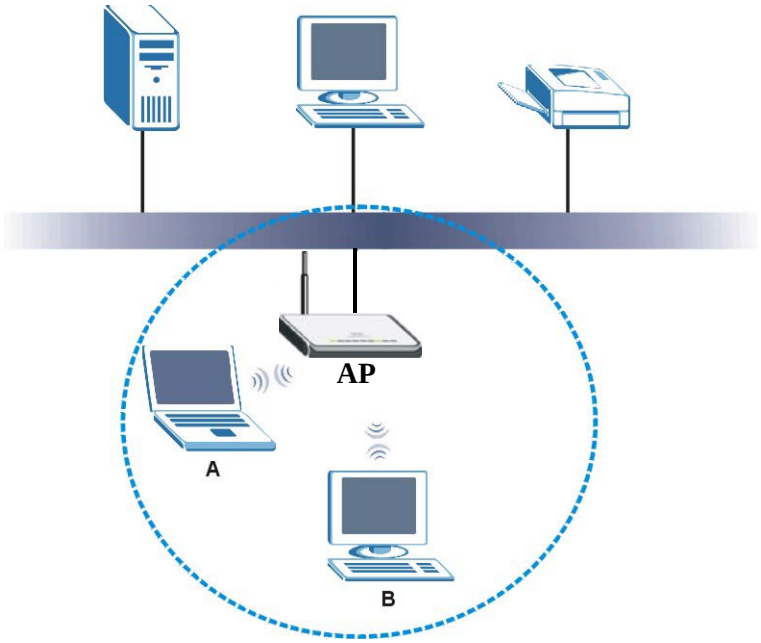
Wireless LAN

7.1 Overview

This chapter discusses how to configure the wireless network settings in your NBG4115. See the appendices for more detailed information about wireless networks.

The following figure provides an example of a wireless network.

Figure 46 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices A and B are called wireless clients. The wireless clients use the access point (AP) to interact with other devices (such as the printer) or with the Internet. Your NBG4115 is the AP.

7.1.1 What You Can Do in this Chapter

- Use the **General** screen (Section 7.2 on page 80) to enable the Wireless LAN, enter the SSID and select the wireless security mode.
- Use the **MAC Filter** screen (Section 7.3 on page 86) to allow or deny wireless stations based on their MAC addresses from connecting to the NBG4115.
- Use the **Advanced** screen (Section 7.4 on page 87) to allow intra-BSS networking and set the RTS/CTS Threshold.
- Use the **QoS** screen (Section 7.5 on page 89) to ensure Quality of Service (QoS) in your wireless network.

- Use the **WPS** screen (Section 7.6 on page 92) to quickly set up a wireless network with strong security, without having to configure security settings manually.
- Use the **WPS Station** screen (Section 7.7 on page 93) to add a wireless station using WPS.
- Use the **Scheduling** screen (Section 7.8 on page 94) to set the times your wireless LAN is turned on and off.

7.1.2 What You Should Know

Every wireless network must follow these basic guidelines.

- Every wireless client in the same wireless network must use the same SSID.

  The SSID is the name of the wireless network. It stands for Service Set IDentity.
- If two wireless networks overlap, they should use different channels.

  Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.
- Every wireless client in the same wireless network must use security compatible with the AP.

  Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

Wireless Security Overview

The following sections introduce different types of wireless security you can set up in the wireless network.

SSID

Normally, the AP acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the AP does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized devices to get the SSID. In addition, unauthorized devices can still see the information that is sent in the wireless network.

MAC Address Filter

Every wireless client has a unique identification number, called a MAC address.[1] A MAC address is usually written using twelve hexadecimal characters[2]; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each wireless client, see the appropriate User's Guide or other documentation.

You can use the MAC address filter to tell the AP which wireless clients are allowed or not allowed to use the wireless network. If a wireless client is allowed to use the wireless network, it still has to have the correct settings (SSID, channel, and security). If a wireless client is not allowed to use the wireless network, it does not matter if it has the correct settings.

1. Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.
2. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized devices to get the MAC address of an authorized wireless client. Then, they can use that MAC address to use the wireless network.

User Authentication

You can make every user log in to the wireless network before they can use it. This is called user authentication. However, every wireless client in the wireless network has to support IEEE 802.1x to do this.

For wireless networks, there are two typical places to store the user names and passwords for each user.

- In the AP: this feature is called a local user database or a local database.
- In a RADIUS server: this is a server used in businesses more than in homes.

If your AP does not provide a local user database and if you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized devices can still see the information that is sent in the wireless network, even if they cannot use the wireless network. Furthermore, there are ways for unauthorized wireless users to get a valid user name and password. Then, they can use that user name and password to use the wireless network.

Local user databases also have an additional limitation that is explained in the next section.

Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

The types of encryption you can choose depend on the type of user authentication. (See Section on page 79 for information about this.)

Table 30 Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION	RADIUS SERVER
Weakest	No Security	WPA
↕	Static WEP	
	WPA-PSK	
Strongest	WPA2-PSK	WPA2

For example, if the wireless network has a RADIUS server, you can choose **WPA** or **WPA2**. If users do not log in to the wireless network, you can choose no encryption, **Static WEP**, **WPA-PSK**, or **WPA2-PSK**.

Usually, you should set up the strongest encryption that every wireless client in the wireless network supports. For example, suppose the AP does not have a local user database, and you do not have a RADIUS server. Therefore, there is no user authentication. Suppose the wireless network has two wireless clients. Device A only supports WEP, and device B supports WEP and WPA. Therefore, you should set up **Static WEP** in the wireless network.

Note: It is recommended that wireless networks use **WPA-PSK**, **WPA**, or stronger encryption. IEEE 802.1x and WEP encryption are better than none at all, but it is still possible for unauthorized devices to figure out the original information pretty quickly.

Note: It is not possible to use **WPA-PSK**, **WPA** or stronger encryption with a local user database. In this case, it is better to set up stronger encryption with no authentication than to set up weaker encryption with the local user database.

When you select **WPA2** or **WPA2-PSK** in your NBG4115, you can also select an option (**WPA Compatible**) to support WPA as well. In this case, if some wireless clients support WPA and some support WPA2, you should set up **WPA2-PSK** or **WPA2** (depending on the type of wireless network login) and select the **WPA Compatible** option in the NBG4115.

Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every wireless client in the wireless network must have the same key.

WPS

WiFi Protected Setup (WPS) is an industry standard specification, defined by the WiFi Alliance. WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Depending on the devices in your network, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (Personal Identification Number) in the devices. Then, they connect and set up a secure network by themselves. See how to set up a secure wireless network using WPS in the Section 6.4 on page 65.

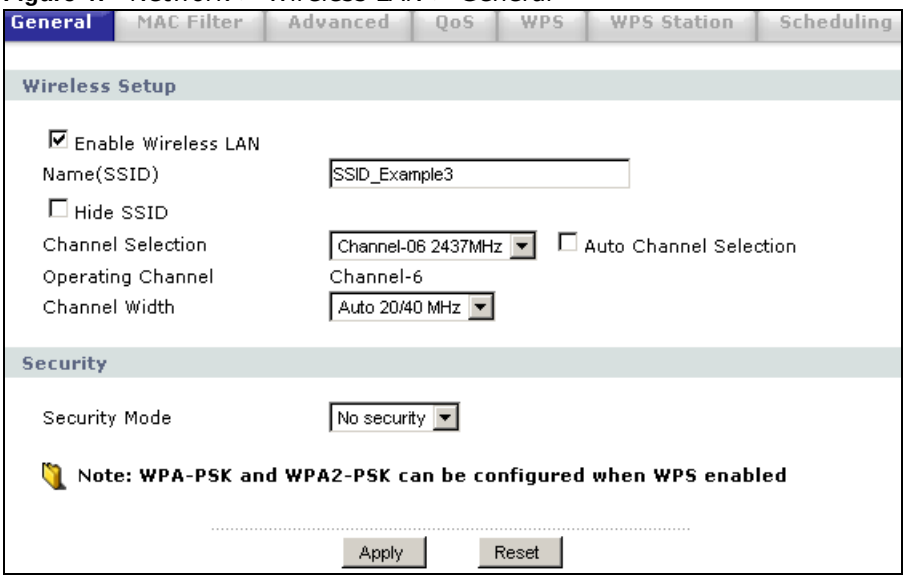
7.2 General

Use this screen to enable the Wireless LAN, enter the SSID and select the wireless security mode.

Note: If you are configuring the NBG4115 from a computer connected to the wireless LAN and you change the NBG4115's SSID, channel or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the NBG4115's new settings.

Click **Network** > **Wireless LAN** to open the **General** screen.

Figure 47 Network > Wireless LAN > General



The following table describes the general wireless LAN labels in this screen.

Table 31 Network > Wireless LAN > General

LABEL	DESCRIPTION
Enable Wireless LAN	Click the check box to activate wireless LAN.
Name(SSID)	(Service Set IDentity) The SSID identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Channel Selection	Set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box. The options vary depending on the frequency band and the country you are in. Refer to the Connection Wizard chapter for more information on channels. This option is only available if **Auto Channel Selection** is disabled.
Auto Channel Selection	Select this check box for the NBG4115 to automatically choose the channel with the least interference. Deselect this check box if you wish to manually select the channel using the **Channel Section** field.
Operating Channel	This displays the channel the NBG4115 is currently using.
Channel Width	Select whether the NBG4115 uses a wireless channel width of 20 or 40 MHz. A standard 20 MHz channel offers transfer speeds of up to 150Mbps whereas a 40MHz channel uses two standard channels and offers speeds of up to 300 Mbps. Because not all devices support 40 MHz channels, select **Auto 20/40MHz** to allow the NBG4115 to adjust the channel bandwidth automatically.

Table 31 Network > Wireless LAN > General

LABEL	DESCRIPTION
Security Mode	Select **WPA-PSK** or **WPA2-PSK** to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as this device. After you select to use a security, additional options appears in this screen. See 7.2.2 and 7.2.3 sections. Or you can select **No Security** to allow any client to associate this network without authentication. Note: If you enable the WPS function, only **No Security**, **WPA-PSK** and **WPA2-PSK** are available in this field.
Apply	Click **Apply** to save your changes back to the NBG4115.
Reset	Click **Reset** to reload the previous configuration for this screen.

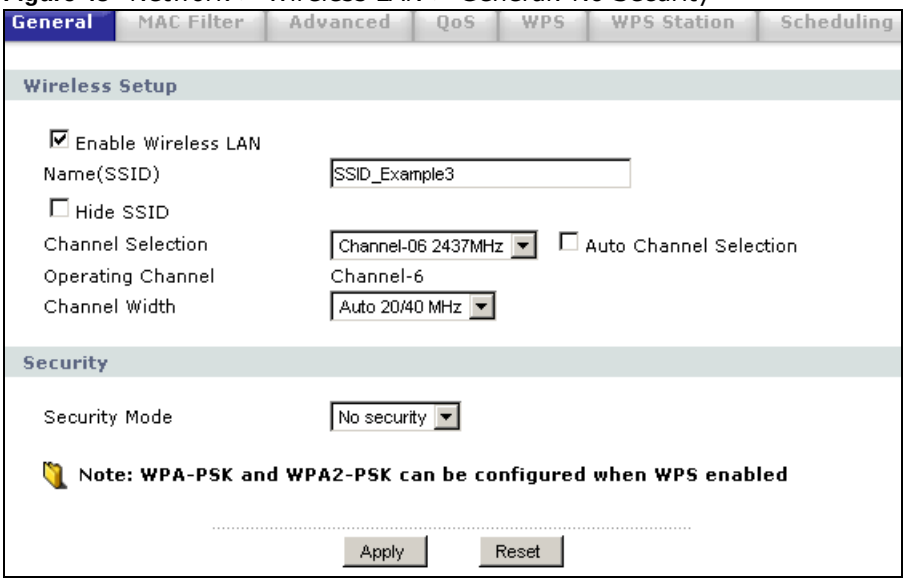
See the rest of this chapter for information on the other labels in this screen.

7.2.1 No Security

Select **No Security** to allow wireless stations to communicate with the access points without any data encryption.

Note: If you do not enable any wireless security on your NBG4115, your network is accessible to any wireless networking device that is within range.

Figure 48 Network > Wireless LAN > General: No Security



The following table describes the labels in this screen.

Table 32 Wireless No Security

LABEL	DESCRIPTION
Security Mode	Choose **No Security** from the drop-down list box.
Apply	Click **Apply** to save your changes back to the NBG4115.
Reset	Click **Reset** to reload the previous configuration for this screen.

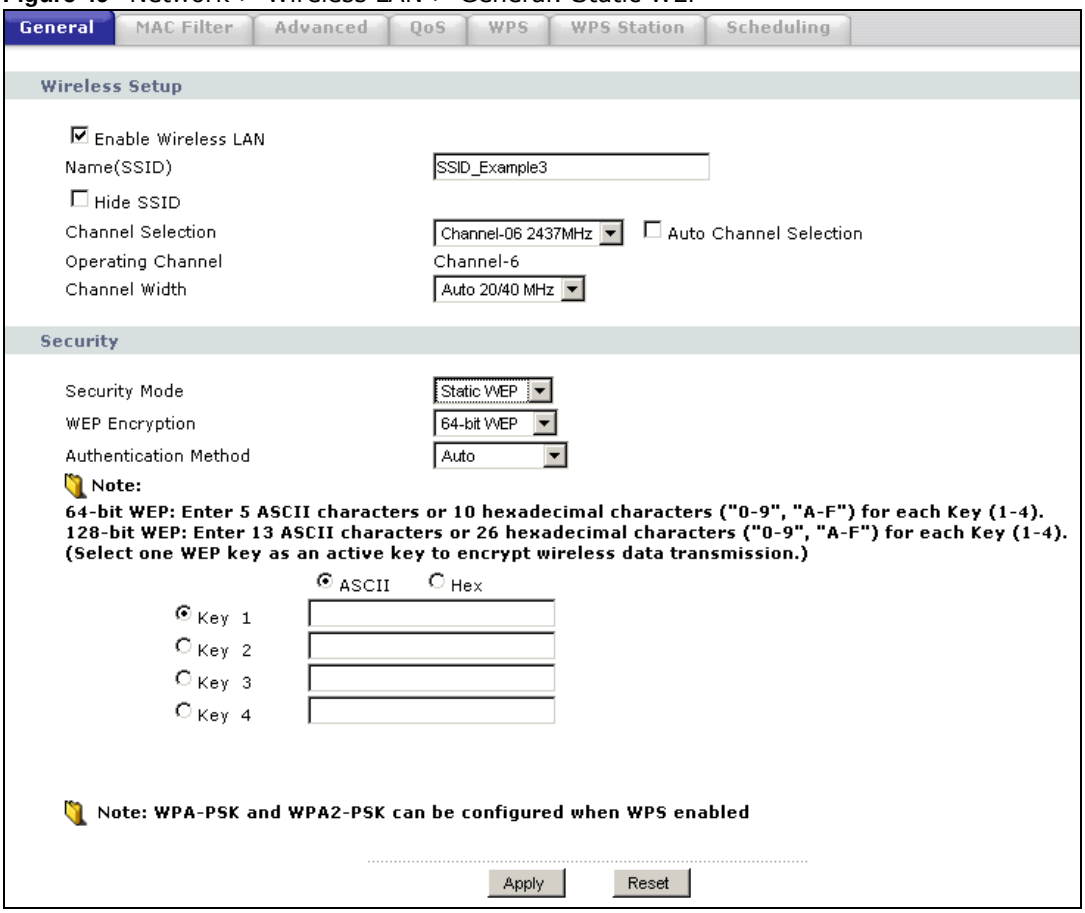
7.2.2 WEP Encryption

WEP encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless stations and the access points must use the same WEP key.

Your NBG4115 allows you to configure up to four 64-bit or 128-bit WEP keys but only one key can be enabled at any one time.

In order to configure and enable WEP encryption; click **Network** > **Wireless LAN** to display the **General** screen. Select **Static WEP** from the **Security Mode** list.

Figure 49 Network > Wireless LAN > General: Static WEP



The following table describes the wireless LAN security labels in this screen.

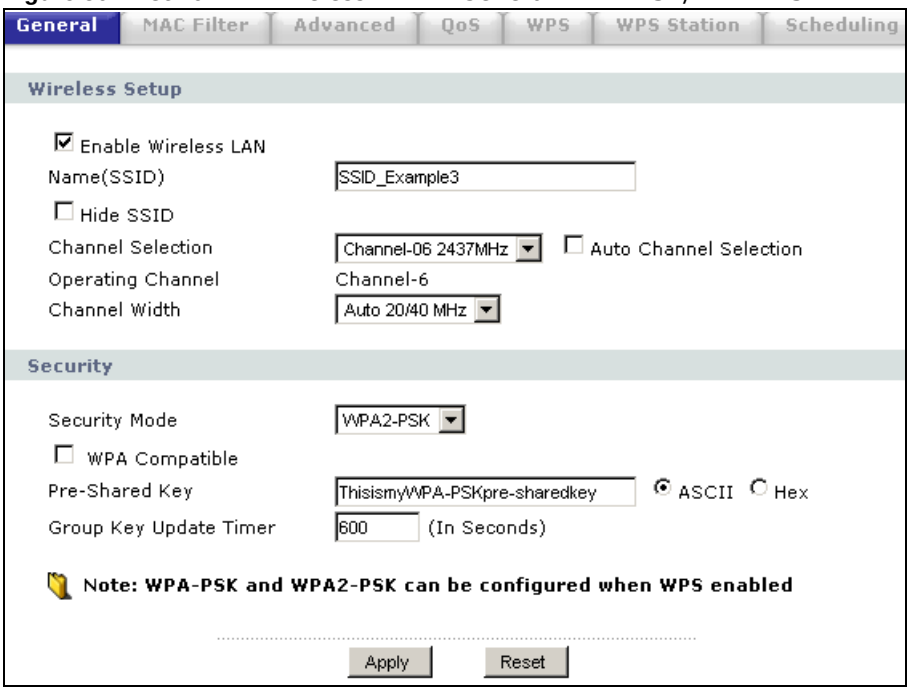
Table 33 Network > Wireless LAN > General: Static WEP

LABEL	DESCRIPTION
WEP Encryption	Select **64-bit WEP** or **128-bit WEP** to enable data encryption.
Authentication Method	This field is activated when you select **64-bit WEP** or **128-bit WEP** in the **WEP Encryption** field. Select **Auto, Open System** or **Shared Key** from the drop-down list box. This field specifies whether the wireless clients have to provide the WEP key to login to the wireless client. Keep this setting at **Auto** or **Open System** unless you want to force a key verification before communication between the wireless client and the ZyXEL Device occurs. Select **Shared Key** to force the clients to provide the WEP key prior to communication.
ASCII	Select this option in order to enter ASCII characters as WEP key.
Hex	Select this option in order to enter hexadecimal characters as a WEP key. The preceding "0x", that identifies a hexadecimal key, is entered automatically.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the NBG4115 and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit WEP**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit WEP**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure at least one key, only one key can be activated at any one time. The default key is key 1.
Apply	Click **Apply** to save your changes back to the NBG4115.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.2.3 WPA-PSK/WPA2-PSK

Click **Network** > **Wireless LAN** to display the **General** screen. Select **WPA-PSK** or **WPA2-PSK** from the **Security Mode** list.

Figure 50 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK



The following table describes the labels in this screen.

Table 34 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK

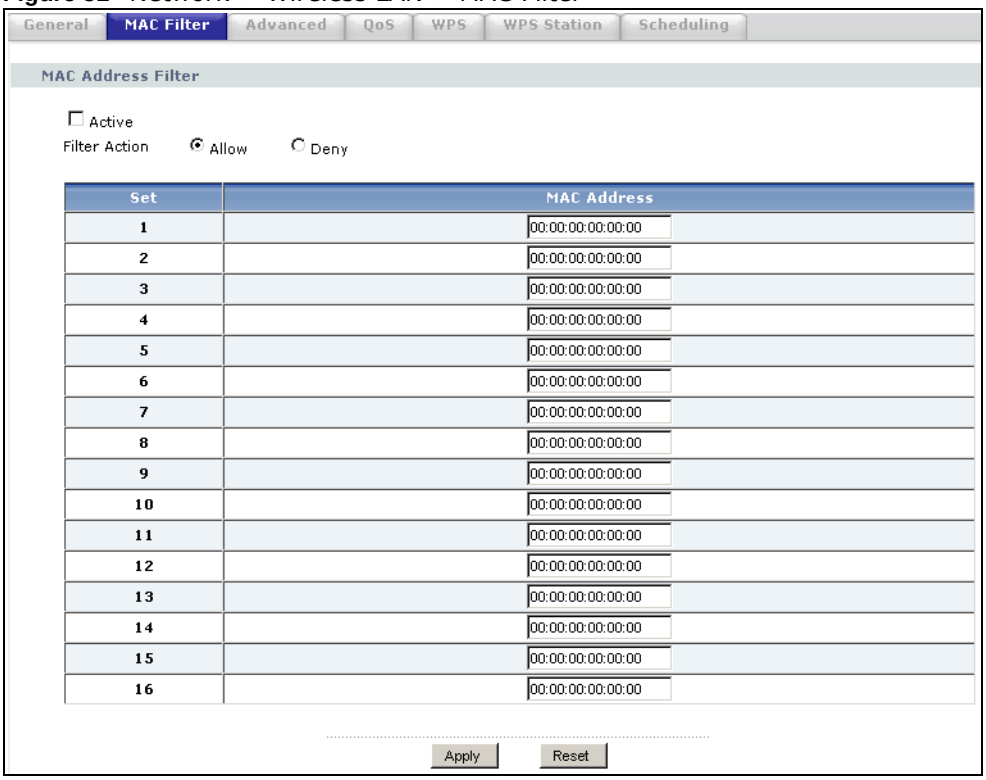
LABEL	DESCRIPTION
WPA Compatible	This check box is available only when you select **WPA2-PSK** in the **Security Mode** field. Select the check box to have both WPA2 and WPA wireless clients be able to communicate with the NBG4115 even when the NBG4115 is using WPA2-PSK.
Pre-Shared Key	**WPA-PSK / WPA2-PSK** uses a simple common password for authentication. Type a pre-shared key from 8 to 63 case-sensitive **ASCII** characters (including spaces and symbols). Type a pre-shared key less than 64 case-sensitive **HEX** characters ("0-9", "A-F").
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP (if using **WPA-PSK / WPA2-PSK** key management) or RADIUS server (if using **WPA / WPA2** key management) sends a new group key out to all clients. The re-keying process is the WPA/WPA2 equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **Group Key Update Timer** is also supported in **WPA-PSK / WPA2-PSK** mode. The default is **1800** seconds (30 minutes).
Apply	Click **Apply** to save your changes back to the NBG4115.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.3 MAC Filter

The MAC filter screen allows you to configure the NBG4115 to give exclusive access to up to 16 devices (Allow) or exclude up to 16 devices from accessing the NBG4115 (Deny). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the devices to configure this screen.

To change your NBG4115's MAC filter settings, click **Network** > **Wireless LAN** > **MAC Filter**. The screen appears as shown.

Figure 51 Network > Wireless LAN > MAC Filter



The following table describes the labels in this menu.

Table 35 Network > Wireless LAN > MAC Filter

LABEL	DESCRIPTION
Active	Select **Yes** from the drop down list box to enable MAC address filtering.
Filter Action	Define the filter action for the list of MAC addresses in the **MAC Address** table. Select **Deny** to block access to the NBG4115, MAC addresses not listed will be allowed to access the NBG4115 Select **Allow** to permit access to the NBG4115, MAC addresses not listed will be denied access to the NBG4115.
Set	This is the index number of the MAC address.
MAC Address	Enter the MAC addresses of the wireless station that are allowed or denied access to the NBG4115 in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.

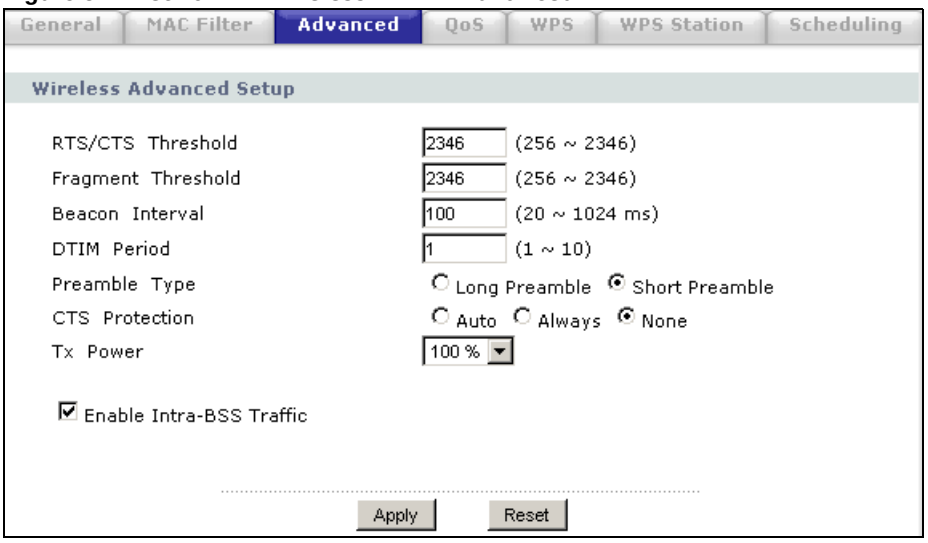
Table 35 Network > Wireless LAN > MAC Filter

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the NBG4115.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.4 Advanced

Click **Network** > **Wireless LAN** > **Advanced**. The screen appears as shown.

Figure 52 Network > Wireless LAN > Advanced



The following table describes the labels in this screen.

Table 36 Network > Wireless LAN > Advanced

LABEL	DESCRIPTION
Wireless Advanced Setup	
RTS/CTS Threshold	Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake. Enter a value between 0 and 2432.
Fragmentation Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter an even number between **256** and **2346**. This field is not available when **Super Mode** is selected.
Beacon Interval	When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again. The interval tells receiving devices on the network how long they can wait in low-power mode before waking up to handle the beacon. This value can be set from 20ms to 1000ms. A high value helps save current consumption of the access point.
DTIM	Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Active Power Management mode. A high DTIM value can cause clients to lose connectivity with the network. This value can be set from 1 to 100.

Table 36 Network > Wireless LAN > Advanced

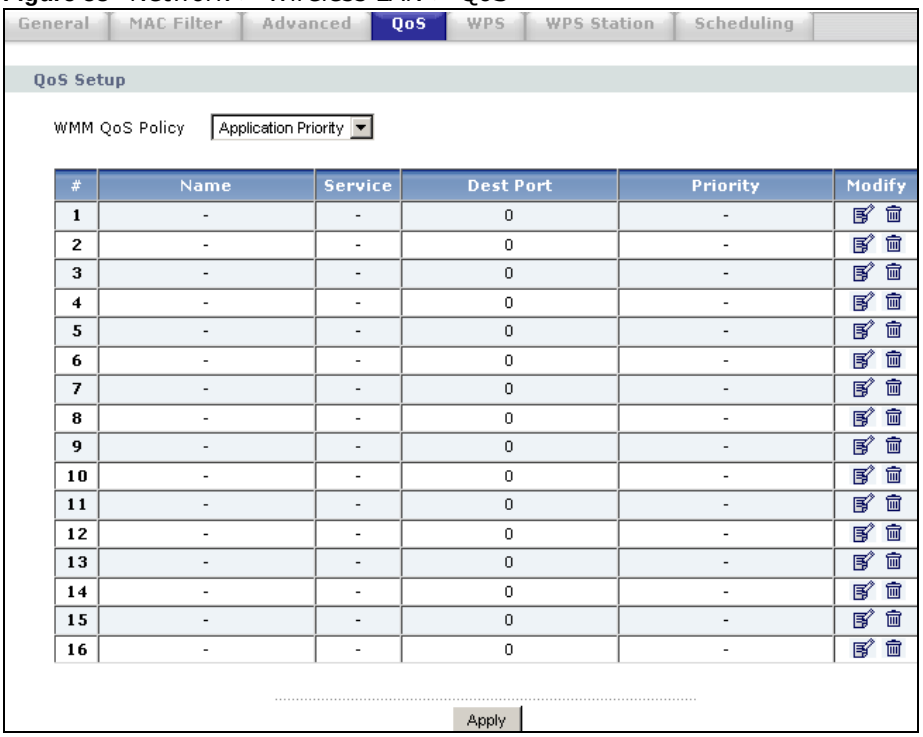
LABEL	DESCRIPTION
Preamble	A preamble affects the timing in your wireless network. There are two preamble modes: long and short. If a device uses a different preamble mode than the NBG4115 does, it cannot communicate with the NBG4115.
CTS Protection	When set to **None**, the NBG4115 protects wireless communication against interference. When set to **Always**, the NBG4115 improves performance within mixed wireless modes. Select **Auto** to let the NBG4115 determine whether to turn this feature on or off in the current environment.
Tx Power	This field controls the transmission power of the NBG4115. When using the NBG4115 with a notebook computer, select a lower transmission power level when you are close to the AP in order to conserve battery power.
Enable Intra-BSS Traffic	A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP). Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client **A** and **B** can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless client **A** and **B** can still access the wired network but cannot communicate with each other.
Apply	Click **Apply** to save your changes back to the NBG4115.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.5 QoS

The QoS screen allows you to automatically give a service (such as e-mail, VoIP or FTP) a priority level.

Click **Network** > **Wireless LAN** > **QoS**. The following screen appears.

Figure 53 Network > Wireless LAN > QoS



The following table describes the labels in this screen.

Table 37 Network > Wireless LAN > QoS

LABEL	DESCRIPTION
WMM QoS Policy	Select **Default** to have the NBG4115 automatically give a service a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly. Select **Application Priority** from the drop-down list box to display a table of application names, services, ports and priorities to which you want to apply WMM QoS. The table appears only if you select **Application Priority** in **WMM QoS Policy**.
#	This is the number of an individual application entry.
Name	This field displays a description given to an application entry.
Service	This field displays either **FTP**, **WWW**, **E-mail** or a **User Defined** service to which you want to apply WMM QoS.
Dest Port	This field displays the destination port number to which the application sends traffic.

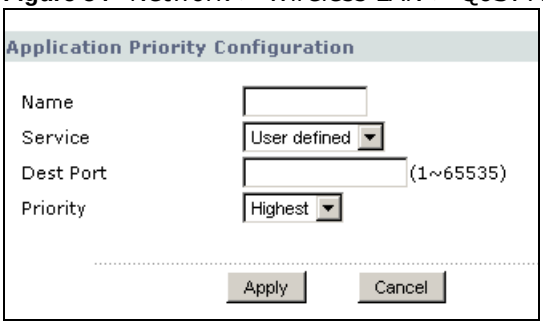
Table 37 Network > Wireless LAN > QoS (continued)

LABEL	DESCRIPTION
Priority	This field displays the priority of the application. **Highest** - Typically used for voice or video that should be high-quality. **High** - Typically used for voice or video that can be medium-quality. **Mid** - Typically used for applications that do not fit into another priority. For example, Internet surfing. **Low** - Typically used for non-critical "background" applications, such as large file transfers and print jobs that should not affect other applications.
Modify	Click the **Edit** icon to open the **Application Priority Configuration** screen. Modify an existing application entry or create an application entry in the **Application Priority Configuration** screen. Click the **Remove** icon to delete an application entry.
Apply	Click **Apply** to save your changes to the NBG4115.

7.5.1 Application Priority Configuration

Use this screen to edit a WMM QoS application entry. Click the edit icon under **Modify**. The following screen displays.

Figure 54 Network > Wireless LAN > QoS: Application Priority Configuration



See Appendix E on page 257 for a list of commonly-used services and destination ports. The following table describes the fields in this screen.

Network > Wireless LAN > QoS: Application Priority Configuration

LABEL	DESCRIPTION
Name	Type a description of the application priority.

Network > Wireless LAN > QoS: Application Priority Configuration (continued)

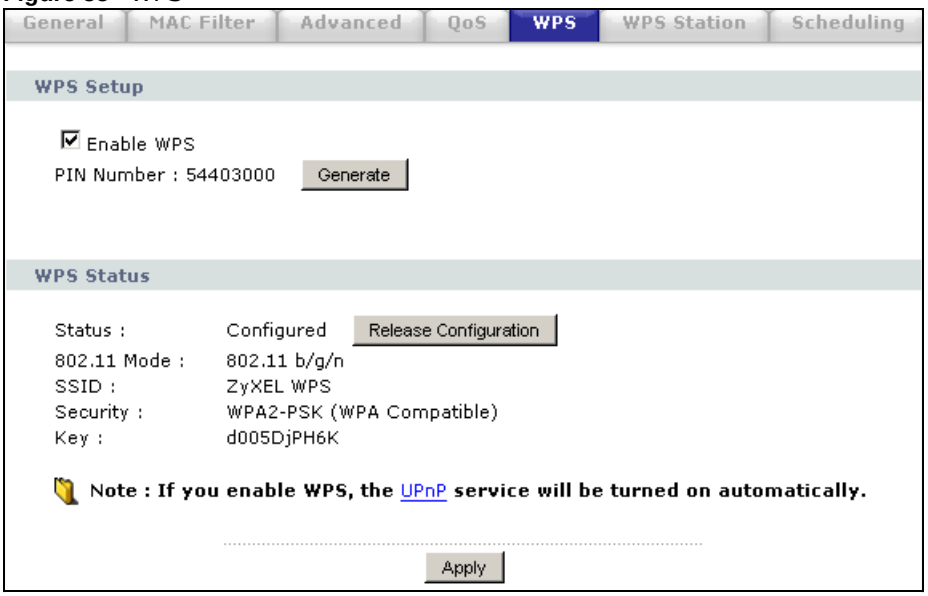
LABEL	DESCRIPTION
Service	The following is a description of the applications you can prioritize with WMM QoS. Select a service from the drop-down list box. • **E-Mail** Electronic mail consists of messages sent through a computer network to specific groups or individuals. Here are some default ports for e-mail: POP3 - port 110 IMAP - port 143 SMTP - port 25 HTTP - port 80 • **FTP** File Transfer Protocol enables fast transfer of files, including large files that it may not be possible to send via e-mail. FTP uses port number 21. • **WWW** The World Wide Web is an Internet system to distribute graphical, hyper-linked information, based on Hyper Text Transfer Protocol (HTTP) - a client/server protocol for the World Wide Web. The Web is not synonymous with the Internet; rather, it is just one service on the Internet. Other services on the Internet include Internet Relay Chat and Newsgroups. The Web is accessed through use of a browser. • **User-Defined** User-defined services are user specific services configured using known ports and applications.
Dest Port	This displays the port the selected service uses. Type a port number in the field provided if you want to use a different port to the default port.
Priority	Select a priority from the drop-down list box.
Apply	Click **Apply** to save your changes back to the NBG4115.
Cancel	Click **Cancel** to return to the previous screen.

7.6 WPS

Use this screen to enable/disable WPS, view or generate a new PIN number and check current WPS status.

To open this screen, click **Network** > **Wireless LAN** > **WPS** tab.

Figure 55 WPS



The following table describes the labels in this screen.

Table 38 WPS

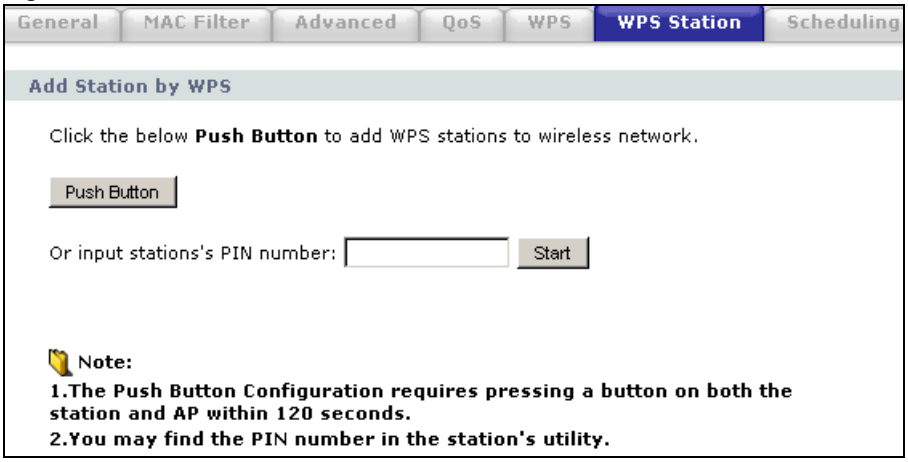
LABEL	DESCRIPTION
WPS Setup	
Enable WPS	Select this to enable the WPS feature.
PIN Number	This displays a PIN number last time system generated. Click **Generate** to generate a new PIN number.
WPS Status	
Status	This displays **Configured** when the NBG4115 has connected to a wireless network using WPS or when **Enable WPS** is selected and wireless or wireless security settings have been changed. The current wireless and wireless security settings also appear in the screen. This displays **Unconfigured** if WPS is disabled and there are no wireless or wireless security changes on the NBG4115 or you click **Release_Configuration** to remove the configured wireless and wireless security settings.
Release Configuration	This button is only available when the WPS status displays **Configured**. Click this button to remove all configured wireless and wireless security settings for WPS connections on the NBG4115.
Apply	Click **Apply** to save your changes back to the NBG4115.
Refresh	Click **Refresh** to get this screen information afresh.

7.7 WPS Station

Use this screen when you want to add a wireless station using WPS. To open this screen, click **Network** > **Wireless LAN** > **WPS Station** tab.

Note: Note: After you click **Push Button** on this screen, you have to press a similar button in the wireless station utility within 2 minutes. To add the second wireless station, you have to press these buttons on both device and the wireless station again after the first 2 minutes.

Figure 56 WPS Station


General
MAC Filter
Advanced
QoS
WPS
WPS Station
Scheduling
Add Station by WPS
Click the below Push Button to add WPS stations to wireless network.
Push Button
Or input stations's PIN number:
Start
Note:
1.The Push Button Configuration requires pressing a button on both the station and AP within 120 seconds.
2.You may find the PIN number in the station's utility.

The following table describes the labels in this screen.

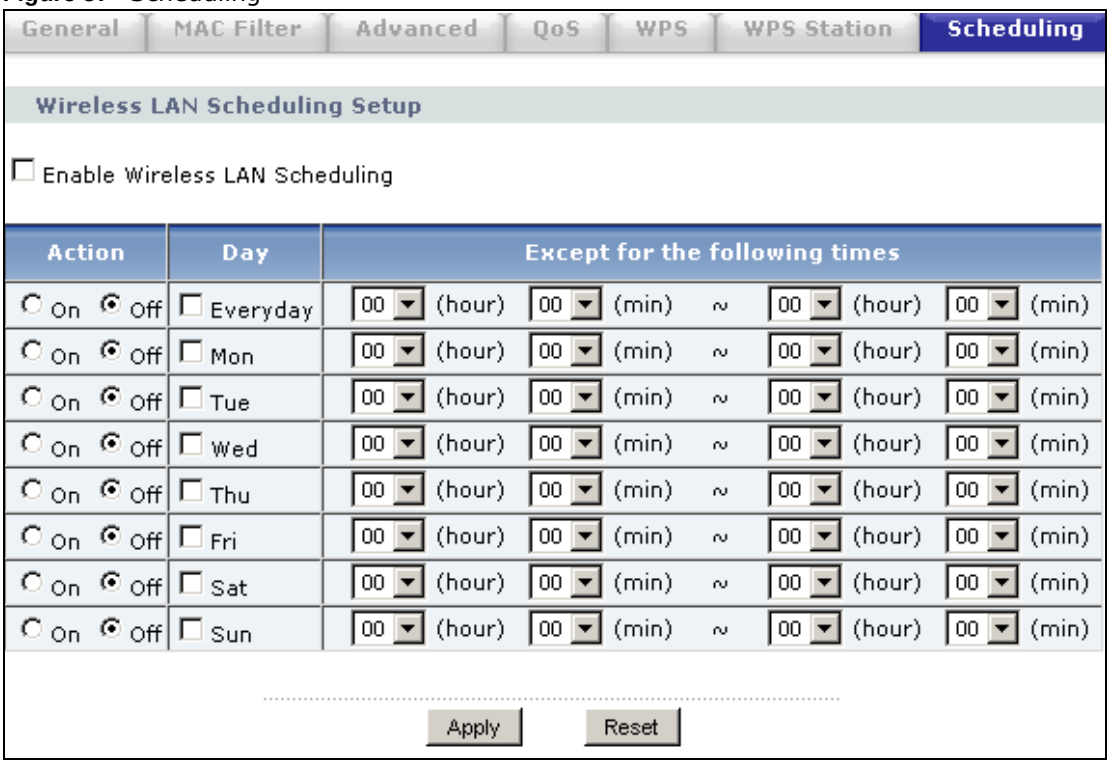
Table 39 WPS Station

LABEL	DESCRIPTION
Push Button	Use this button when you use the PBC (Push Button Configuration) method to configure wireless stations's wireless settings. See Section 6.4.1 on page 66. Click this to start WPS-aware wireless station scanning and the wireless security information synchronization.
Or input station's PIN number	Use this button when you use the PIN Configuration method to configure wireless station's wireless settings. See Section 6.4.2 on page 67. Type the same PIN number generated in the wireless station's utility. Then click **Start** to associate to each other and perform the wireless security information synchronization.

7.8 Scheduling

Use this screen to set the times your wireless LAN is turned on and off. Wireless LAN scheduling is disabled by default. The wireless LAN can be scheduled to turn on or off on certain days and at certain times. To open this screen, click **Network** > **Wireless LAN** > **Scheduling** tab.

Figure 57 Scheduling


General
MAC Filter
Advanced
QoS
WPS
WPS Station
Scheduling
Wireless LAN Scheduling Setup
Enable Wireless LAN Scheduling
Action
Day
Except for the following times
On Off Everyday 00 (hour) 00 (min) ~ 00 (hour) 00 (min)
On Off Mon 00 (hour) 00 (min) ~ 00 (hour) 00 (min)
On Off Tue 00 (hour) 00 (min) ~ 00 (hour) 00 (min)
On Off Wed 00 (hour) 00 (min) ~ 00 (hour) 00 (min)
On Off Thu 00 (hour) 00 (min) ~ 00 (hour) 00 (min)
On Off Fri 00 (hour) 00 (min) ~ 00 (hour) 00 (min)
On Off Sat 00 (hour) 00 (min) ~ 00 (hour) 00 (min)
On Off Sun 00 (hour) 00 (min) ~ 00 (hour) 00 (min)
Apply
Reset

The following table describes the labels in this screen.

Table 40 Scheduling

LABEL	DESCRIPTION
Enable Wireless LAN Scheduling	Select this to enable Wireless LAN scheduling.
Action	Select **On** or **Off** to specify whether the Wireless LAN is turned on or off. This field works in conjunction with the **Day** and **Except for the following times** fields.
Day	Select **Everyday** or the specific days to turn the Wireless LAN on or off. If you select **Everyday** you can not select any specific days. This field works in conjunction with the **Except for the following times** field.
Except for the following times (24-Hour Format)	Select a begin time using the first set of **hour** and minute (**min**) drop down boxes and select an end time using the second set of **hour** and minute (**min**) drop down boxes. If you have chosen **On** earlier for the WLAN Status the Wireless LAN will turn off between the two times you enter in these fields. If you have chosen **Off** earlier for the WLAN Status the Wireless LAN will turn on between the two times you enter in these fields. Note: Entering the same begin time and end time will mean the whole day.
Apply	Click **Apply** to save your changes back to the NBG4115.
Reset	Click **Reset** to reload the previous configuration for this screen.

8 WAN

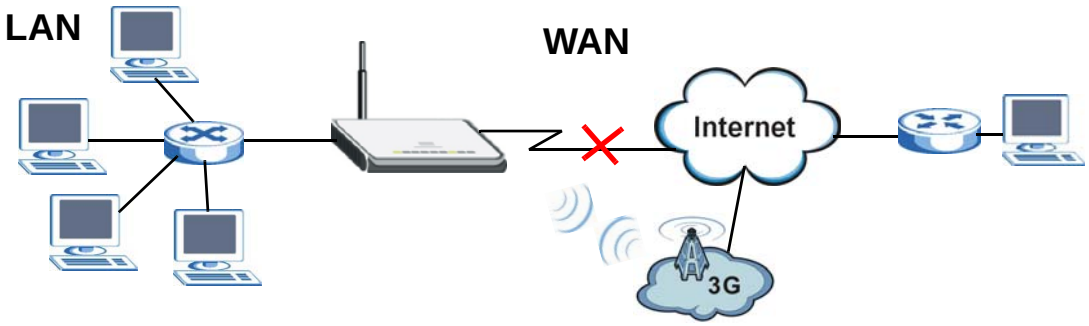
8.1 Overview

This chapter discusses the NBG4115's **WAN** screens. Use these screens to configure your NBG4115 for Internet access.

A WAN (Wide Area Network) connection is an outside connection to another network or the Internet. It connects your private networks (such as a LAN (Local Area Network) and other networks, so that a computer in one location can communicate with computers in other locations.

The NBG4115 also supports a 3G WAN connection. You can use 3G as your primary WAN or use the 3G WAN connection as a backup.

Figure 58 WAN Backup



See the chapter about the connection wizard for more information on the fields in the WAN screens.

8.2 What You Can Do in this Chapter

- Use the **Internet Connection** (Section 8.4 on page 102) screen to enter your ISP information and set how the computer acquires its IP, DNS and WAN MAC addresses. This screen is not available when you select the **Fixed 3G Router Mode** option in the **NetUSB > General** screen.
- Use the **General** (Section 8.4 on page 102) screen to configure WAN priority, the action the NBG4115 takes after the primary WAN interface fails, and connection test settings for the NBG4115. This screen is available only when you select the **Fixed 3G Router Mode** option in the **NetUSB > General** screen.
- Use the **WAN1** (Section 8.4 on page 102) screen to configure the WAN1 interface for Internet access on the NBG4115. This screen is available only when you select the **Fixed 3G Router Mode** option in the **NetUSB > General** screen.
- Use the **3G(WAN2)** (Section 8.4 on page 102) screen to configure the WAN2 interface for Internet access on the NBG4115. This screen is available only when you select the **Fixed 3G Router Mode** option in the **NetUSB > General** screen.

- Use the **Advanced** (Section 8.5 on page 110) screen to enable multicasting, configure Windows networking and bridge.

8.2.1 What You Need To Know

The following terms and concepts may help as you read through this chapter.

Encapsulation Method

Encapsulation is used to include data from an upper layer protocol into a lower layer protocol. To set up a WAN connection to the Internet, you need to use the same encapsulation method used by your ISP (Internet Service Provider). If your ISP offers a dial-up Internet connection using PPPoE (PPP over Ethernet) or PPTP (Point-to-Point Tunneling Protocol), they should also provide a username and password (and service name) for user authentication.

WAN IP Address

The WAN IP address is an IP address for the NBG4115, which makes it accessible from an outside network. It is used by the NBG4115 to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the NBG4115 tries to access the Internet.

If your ISP assigns you a static WAN IP address, they should also assign you the subnet mask and DNS server IP address(es) (and a gateway IP address if you use the Ethernet or ENET ENCAP encapsulation method).

DNS Server Address Assignment

Use Domain Name System (DNS) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.zyxel.com is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The NBG4115 can get the DNS server addresses in the following ways.

1. The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.
2. If your ISP dynamically assigns the DNS server IP addresses (along with the NBG4115's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

WAN MAC Address

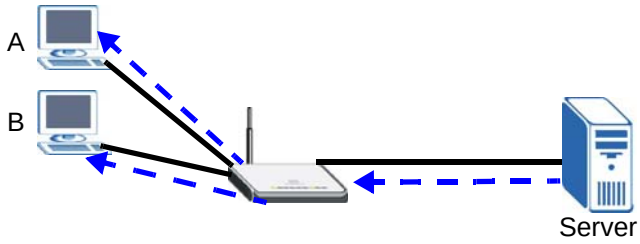
The MAC address screen allows users to configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Choose **Factory Default** to select the factory assigned default MAC Address.

Otherwise, click **Clone the computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to configuration file. It is recommended that you clone the MAC address prior to hooking up the WAN Port.

Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

Figure 59 Multicast Example



In the multicast example above, systems A and B comprise one multicast group. In multicasting, the server only needs to send one data stream and this is delivered to systems A and B.

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group - it is not used to carry user data. The NBG4115 supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**).

At start up, the NBG4115 queries all directly connected networks to gather group membership. After that, the NBG4115 periodically updates this information. IP multicasting can be enabled/ disabled on the NBG4115 LAN and/or WAN interfaces in the Web Configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

NetBIOS over TCP/IP

NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN.

Maximum Transmission Unit

A maximum transmission unit (MTU) is the largest size packet or frame, specified in octets (eight-bit bytes) that can be sent in a packet- or frame-based network. The Transmission Control Protocol (TCP) uses the MTU to determine the maximum size of each packet in any transmission. Too large an MTU size may mean retransmissions if the packet encounters a router that can't handle that large a packet. Too small an MTU size means relatively more header overhead and more acknowledgements that have to be sent and handled.

Auto-Bridge

In the rear panel of your NBG4115, you can see two LAN ports (1 to 2) and one WAN port. The WAN port is for your Internet access connection, and the LAN ports are for your network devices. The WAN port has a different IP address from the LAN ports.

When you enable auto-bridging in your NBG4115, all three ports (2 LAN ports and the WAN port) share the same IP address. This might happen if you put the NBG4115 behind a NAT router that assigns it this IP address. When the NBG4115 is in auto-bridge mode, the NBG4115 acts as an AP

and all the interfaces (LAN, WAN and WLAN) are bridged. In this mode, your NAT, DHCP server and firewall on the NBG4115 are not available. You do not have to reconfigure them if you return to router mode.

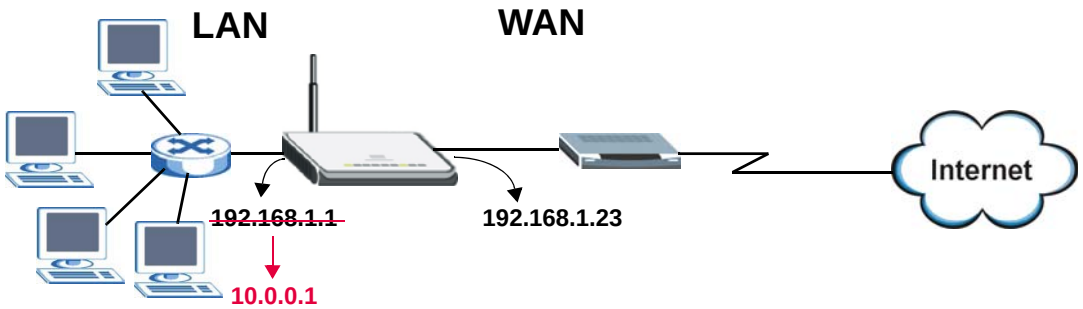
Auto-bridging only works under the following conditions:

- The WAN IP must be 192.168.x.y (where x and y must be from zero to nine). If the LAN IP address and the WAN IP address are in the same subnet but x or y is greater than nine, the device operates in router mode (with firewall available).
- The device must be in **Router Mode** (see Chapter 24 on page 181 for more information) for auto-bridging to become active.

Auto-IP-Change

When the NBG4115 gets a WAN IP address which is in the same subnet as the LAN IP address 192.168.1.1, Auto-IP-Change allows the NBG4115 to change its LAN IP address to 10.0.0.1 automatically. If the NBG4115's original LAN IP address is 10.0.0.1 and the WAN IP address is in the same subnet, such as 10.0.0.3, the NBG4115 switches to use 192.168.1.1 as its LAN IP address.

Figure 60 Auto-IP-Change



Auto-IP-Change only works under the following conditions:

- The NBG4115 must be in **Router Mode** (see Chapter 24 on page 181 for more information) for Auto-IP-Change to become active.
- The NBG4115 is set to receive a dynamic WAN IP address using the Ethernet, PPPoE or PPTP connection type.

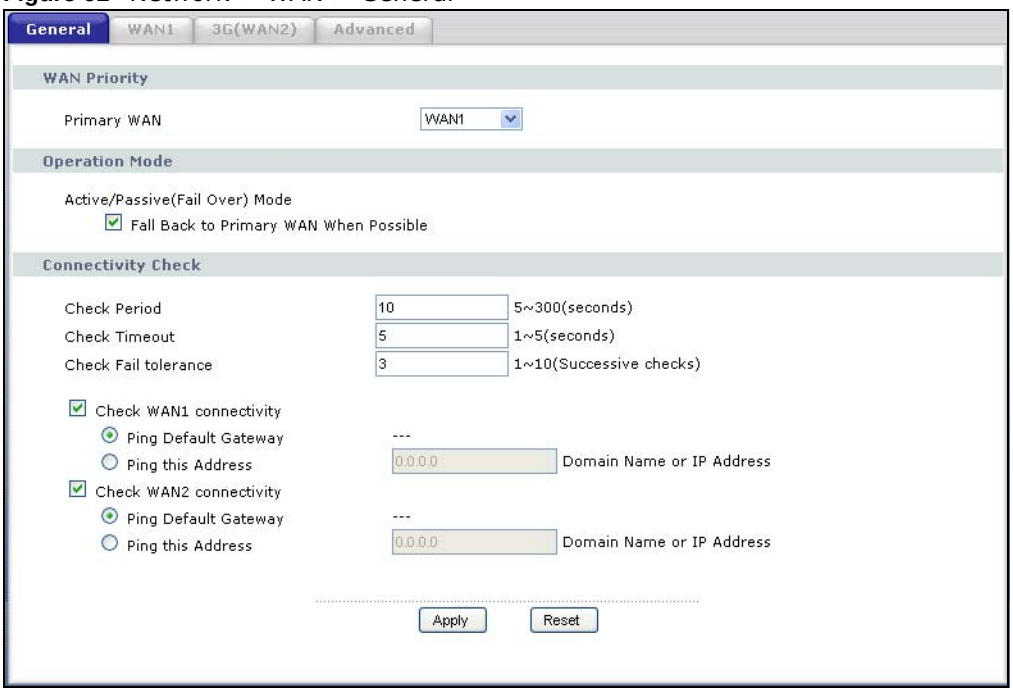
8.3 The General Screen

Use this screen to configure WAN priority, the action the NBG4115 takes after the primary WAN interface fails, and connection test properties.

This screen is available only when you select the **Fixed 3G Router Mode** option in the **NetUSB > General** screen.

Click **Network** > **WAN** > **General**. The screen appears as shown.

Figure 61 Network > WAN > General



The following table describes the labels in this screen.

Table 41 Network > WAN > General

LABEL	DESCRIPTION
WAN Priority	
Primary WAN	Use this field to configure which WAN interface has the highest priority and the NBG4115 uses it as the primary WAN interface. **WAN1** refers to the physical WAN port and **3G(WAN2)** refers to the 3G wireless adapter connected to the USB port on the NBG4115.
Operation Mode	
Active/Passive(Fail Over) Mode	The NBG4115 uses the second highest priority WAN interface as a back up. This means that the NBG4115 will normally use the highest priority (primary) WAN interface (depending on the priority you configure in the **Primary WAN** fields). The NBG4115 will switch to the secondary (second highest priority) WAN interface when the primary WAN interface's connection fails.
Fall Back to Primary WAN When Possible	This field determines the action the NBG4115 takes after the primary WAN interface fails and the NBG4115 starts using the secondary WAN interface. Select this check box to have the NBG4115 change back to using the primary WAN interface when the NBG4115 can connect through the primary WAN interface again. Clear this check box to have the NBG4115 continue using the secondary WAN interface, even after the NBG4115 can connect through the primary WAN interface again. The NBG4115 continues to use the secondary WAN interface until it's connection fails (at which time it will change back to using the primary WAN interface if its connection is up.
Connectivity Check	

Table 41 Network > WAN > General (continued)

LABEL	DESCRIPTION
Check Period	The NBG4115 tests a WAN connection by periodically sending a ping to either the default gateway or the address in the **Ping this Address** field. Type a number of seconds (5 to 300) to set the time interval between checks. Allow more time if your destination IP address handles lots of traffic.
Check Timeout	Type the number of seconds (1 to 10) for your NBG4115 to wait for a response to the ping before considering the check to have failed. This setting must be less than the **Check Period**. Use a higher value in this field if your network is busy or congested.
Check Fail Tolerance	Type how many WAN connection checks can fail (1 to 10) before the connection is considered "down" (not connected). The NBG4115 still checks a "down" connection to detect if it reconnects.
Check WAN1/2 connectivity	Select the check box to have the NBG4115 periodically test the respective WAN interface's connection. Select **Ping Default Gateway** to have the NBG4115 ping the WAN interface's default gateway IP address. Select **Ping this Address** and enter a domain name or IP address of a reliable nearby computer (for example, your ISP's DNS server address) to have the NBG4115 ping that address. For a domain name, use up to 63 alphanumeric characters (hyphens, periods and the underscore are also allowed) without spaces.
Apply	Click **Apply** to save your changes back to the NBG4115.
Reset	Click **Reset** to begin configuring this screen afresh.

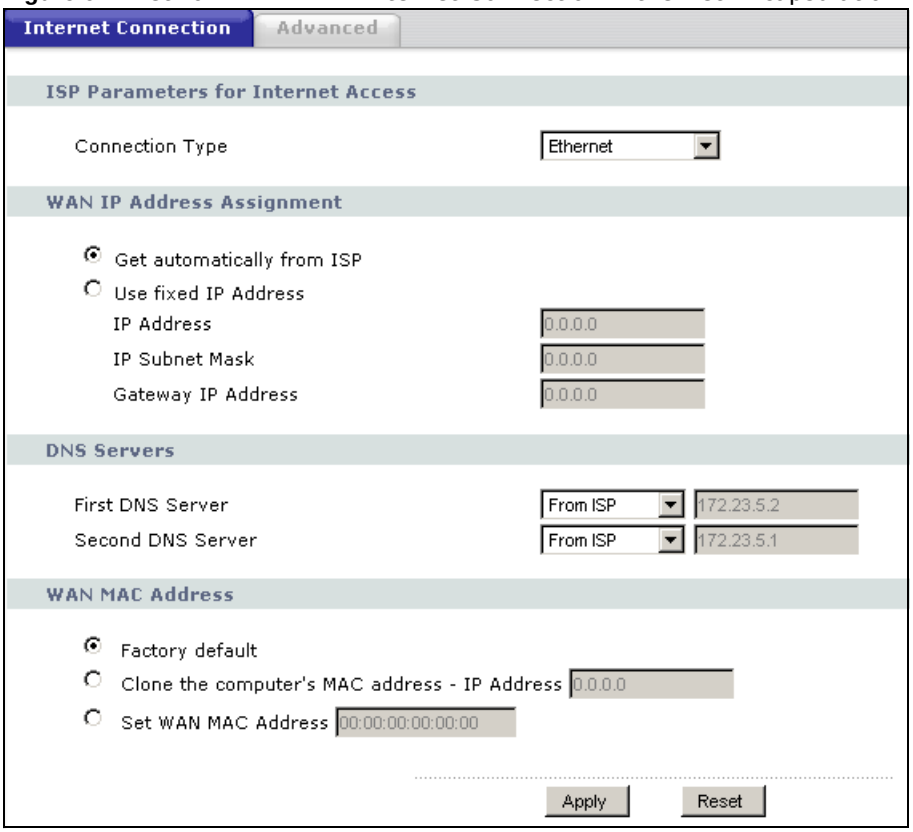
8.4 The WAN1 Internet Connection Screen

Use this screen to change your NBG4115's Internet access settings for a wired WAN connection. Click **Network** > **WAN** or click **Network** > **WAN > WAN1** if you select the **Fixed 3G Router Mode** option in the **NetUSB > General** screen. The screen differs according to the connection you choose.

8.4.1 Ethernet

This screen displays when you select the **Ethernet** connection type.

Figure 62 Network > WAN > Internet Connection: Ethernet Encapsulation



The following table describes the labels in this screen.

Table 42 Network > WAN > Internet Connection: Ethernet

LABEL	DESCRIPTION
Connection Type	You must choose the **Ethernet** option when the WAN port is used as a regular Ethernet.
WAN IP Address Assignment	
Get automatically from ISP	Select this option if the ISP or your network administrator did not assign a static IP address to use for Internet access.
Use Fixed IP Address	Select this option if you were assigned a fixed IP address (and DNS server settings) to use for Internet access
IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address**.
IP Subnet Mask	Enter the **IP Subnet Mask** in this field.
Gateway IP Address	Enter a **Gateway IP Address** in this field.
DNS Servers	

Table 42 Network > WAN > Internet Connection: Ethernet

LABEL	DESCRIPTION
First DNS Server Second DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the NBG4115's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by either using the NBG4115's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select **Factory default** to use the factory assigned default MAC Address.
Clone the computer's MAC address - IP Address	Select **Clone the computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file. It will not change unless you change the setting or upload a different ROM file.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Apply	Click **Apply** to save your changes back to the NBG4115.
Reset	Click **Reset** to begin configuring this screen afresh.

8.4.2 PPPoE

The NBG4115 supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The **PPP over Ethernet** option is for a dial-up connection using PPPoE.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example Radius).

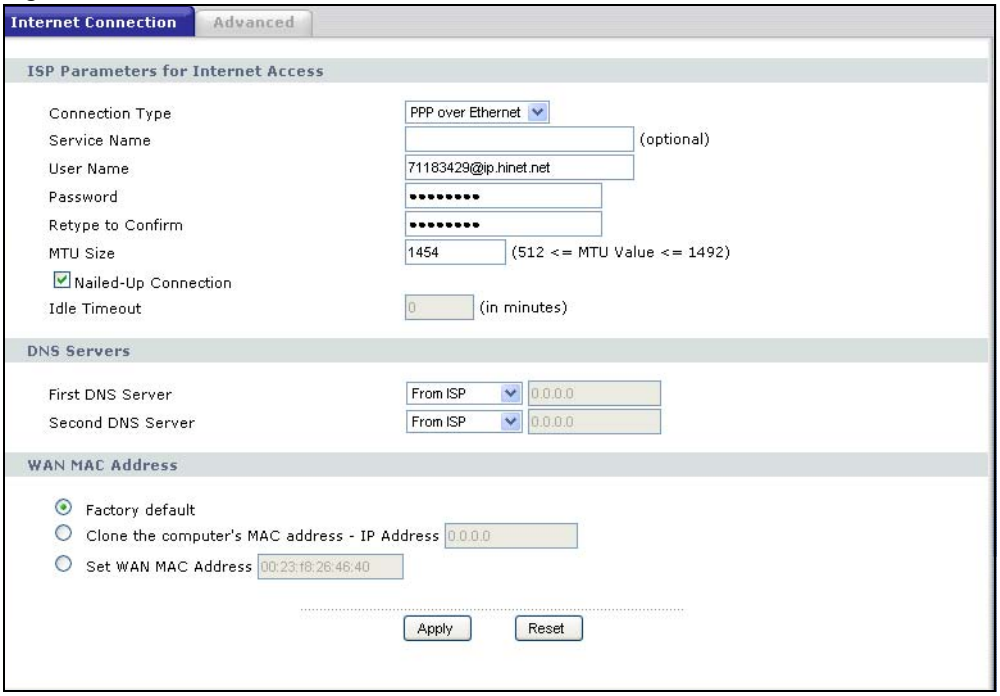
One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the NBG4115 (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the NBG4115 does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

This screen displays when you select the **PPPoE** connection type.

Figure 63 Network > WAN > Internet Connection: PPPoE



The following table describes the labels in this screen.

Table 43 Network > WAN > Internet Connection: PPPoE

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Connection Type	Select **PPP over Ethernet** if you connect to your Internet via dial-up.
Service Name	Type the PPPoE service name provided to you. PPPoE uses a service name to identify and reach the PPPoE server.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
MTU Size	Enter the MTU (Maximum Transfer Unit) size for PPPoE traffic.
Nailed-Up Connection	Select **Nailed-Up Connection** if you do not want the connection to time out.
Idle Timeout	This value specifies the time in minutes that elapses before the router automatically disconnects from the PPPoE server.
DNS Servers	

Table 43 Network > WAN > Internet Connection: PPPoE

LABEL	DESCRIPTION
First DNS Server Second DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the NBG4115's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by using the NBG4115's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select **Factory default** to use the factory assigned default MAC Address.
Clone the computer's MAC address - IP Address	Select **Clone the computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file. It will not change unless you change the setting or upload a different ROM file.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Apply	Click **Apply** to save your changes back to the NBG4115.
Reset	Click **Reset** to begin configuring this screen afresh.

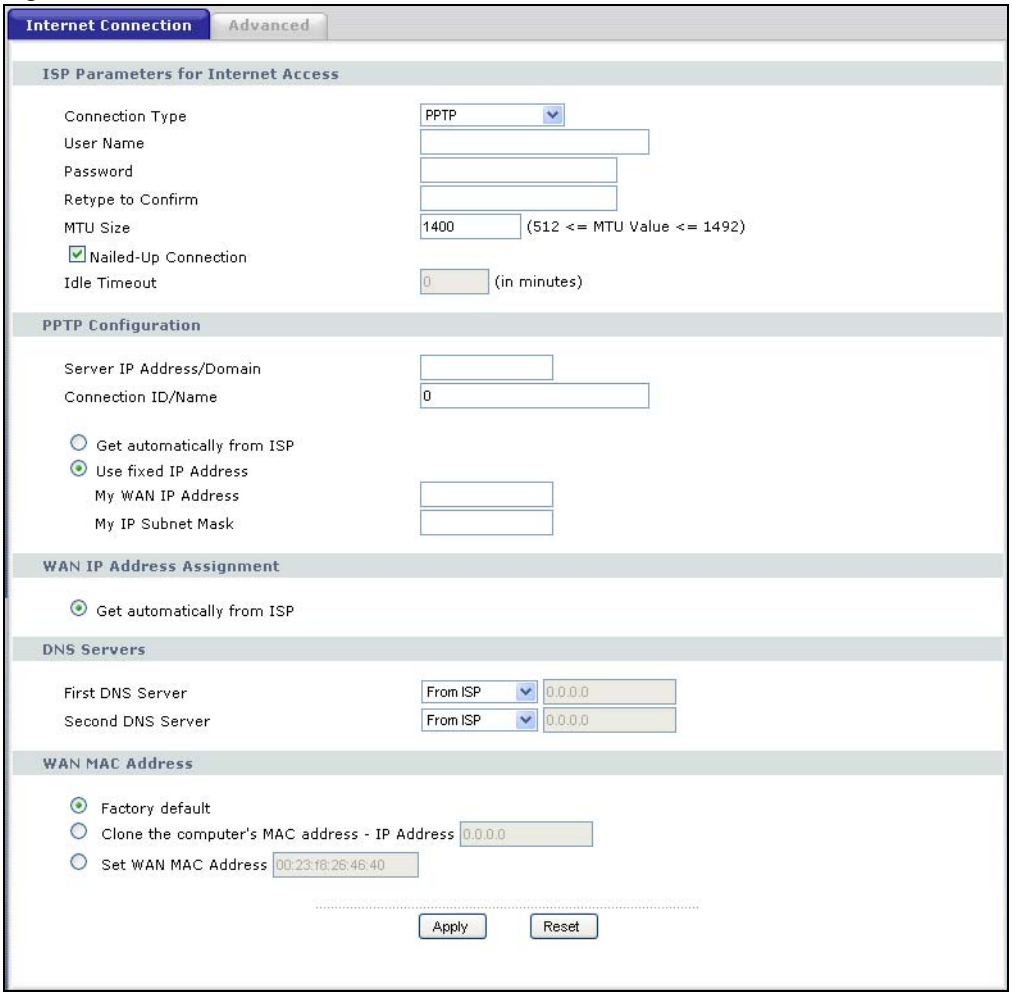
8.4.3 PPTP

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet.

This screen displays when you select the **PPTP** connection type.

Figure 64 Network > WAN > Internet Connection: PPTP



The following table describes the labels in this screen.

Table 44 Network > WAN > Internet Connection: PPTP

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Connection Type	Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks. PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet. The NBG4115 supports only one PPTP server connection at any given time. To configure a PPTP client, you must configure the **User Name** and **Password** fields for a PPP connection and the PPTP parameters for a PPTP connection.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
MTU Size	Enter the MTU (Maximum Transfer Unit) size for PPTP traffic.

Table 44 Network > WAN > Internet Connection: PPTP

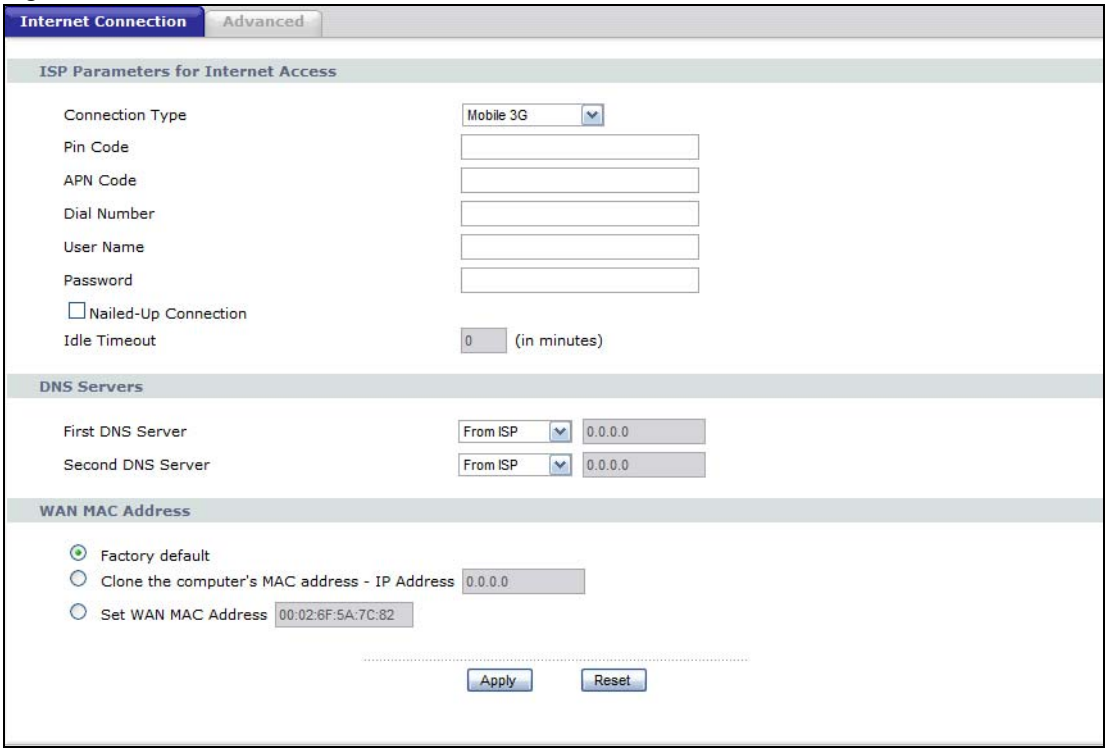
LABEL	DESCRIPTION
Nailed-up Connection	Select **Nailed-Up Connection** if you do not want the connection to time out.
Idle Timeout	This value specifies the time in minutes that elapses before the NBG4115 automatically disconnects from the PPTP server.
PPTP Configuration	
Server IP Address/ Domain	Type the IP address of the PPTP server.
Connection ID/Name	Type your identification name for the PPTP server.
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address**.
My IP Subnet Mask	Your NBG4115 will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the NBG4115.
WAN IP Address Assignment	
Get automatically from ISP	Select this to get your WAN IP address from your ISP.
DNS Servers	
First DNS Server Second DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the NBG4115's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by either using the NBG4115's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select **Factory default** to use the factory assigned default MAC Address.
Clone the computer's MAC address - IP Address	Select **Clone the computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file. It will not change unless you change the setting or upload a different ROM file.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Apply	Click **Apply** to save your changes back to the NBG4115.
Reset	Click **Reset** to begin configuring this screen afresh.

8.4.4 Mobile 3G

3G is an International Telecommunication Union (ITU) mobile networking standard that provides high-speed connectivity, greater network capacity, and a significantly improved broadcast range to compatible devices.

This screen displays when you select the **Mobile 3G** connection type or click **Network** > **WAN > 3G(WAN2)** if you select the **Fixed 3G Router Mode** option in the **NetUSB > General** screen.

Figure 65 Network > WAN > Internet Connection: Mobile 3G



The following table describes the labels in this screen.

Table 45 Network > WAN > Internet Connection: Mobile 3G

LABEL	DESCRIPTION
WAN2 Setup This section is available only when you select the **Fixed 3G Router Mode** option in the **NetUSB > General** screen and click **Network > WAN > 3G(WAN2)**.	
Enable	Select this option to enable WAN 2.
ISP Parameters for Internet Access	
Connection Type	3G (Third Generation) is a digital, packet-switched wireless technology. Bandwidth usage is optimized as multiple users share the same channel and bandwidth is only allocated to users when they send data. It allows fast transfer of voice and non-voice data and provides broadband Internet access to mobile devices. To configure a **Mobile 3G** client, you must configure the **User Name** and **Password** fields as well as **PIN Code**, **APN Code**, and **Dial Number**. This field is not available in the **WAN > 3G(WAN2)** screen.
PIN Code	Enter the 4-digit 3G account PIN code given to you by your ISP.
APN Code	Enter the Access Point Name (APN) given to you by your ISP.
Dial Number	Enter the phone number that must be dialed in order to login to your 3G account from the NBG4115.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.

Table 45 Network > WAN > Internet Connection: Mobile 3G

LABEL	DESCRIPTION
Nailed-up Connection	Select **Nailed-Up Connection** if you do not want the connection to time out.
Idle Timeout	This value specifies the time in minutes that elapses before the NBG4115 automatically disconnects from the PPTP server.
DNS Servers	
First DNS Server Second DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the NBG4115's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by either using the NBG4115's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select **Factory default** to use the factory assigned default MAC Address.
Clone the computer's MAC address - IP Address	Select **Clone the computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file. It will not change unless you change the setting or upload a different ROM file.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Apply	Click **Apply** to save your changes back to the NBG4115.
Reset	Click **Reset** to begin configuring this screen afresh.

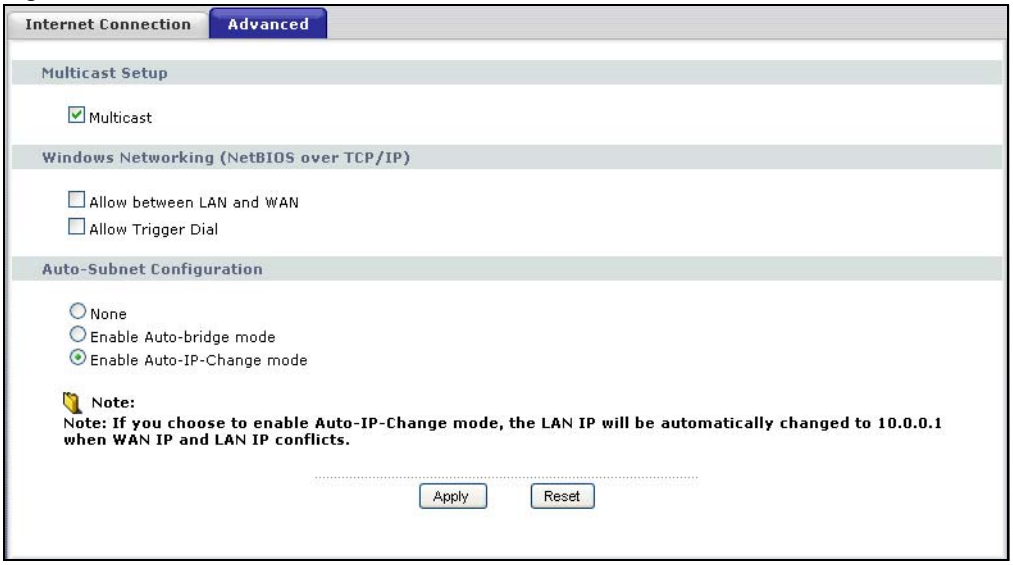
8.5 The Advanced Screen

Use this screen to enable **Multicast**, allow **Windows Networking** and enable **Auto-bridge** or **Auto-IP-Change**.

Note: The three categories shown in this screen are independent of each other.

To change your NBG4115's advanced WAN settings, click **Network** > **WAN** > **Advanced**. The screen appears as shown.

Figure 66 Network > WAN > Advanced



The following table describes the labels in this screen.

Table 46 WAN > Advanced

LABEL	DESCRIPTION
Multicast Setup	
Multicast	Check this to enable multicasting. This applies to traffic routed from the WAN to the LAN. Leaving this blank may cause incoming traffic to be dropped or sent to all connected network devices.
Windows Networking (NetBIOS over TCP/IP)	
Allow between LAN and WAN	Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.
Allow Trigger Dial	Select this option to allow NetBIOS packets to initiate calls.
Auto-Subnet Configuration	
None	Select this option to have the NBG4115 do nothing when it gets a WAN IP address in the range of 192.168.x.y (where x and y are from zero to nine) or in the same subnet as the LAN IP address.
Enable Auto-bridge mode	Select this option to have the NBG4115 switch to bridge mode automatically when the NBG4115 gets a WAN IP address in the range of 192.168.x.y (where x and y are from zero to nine) no matter what the LAN IP address is. The NAT, DHCP server and firewall functions on the NBG4115 are not available in this mode.

Table 46 WAN > Advanced

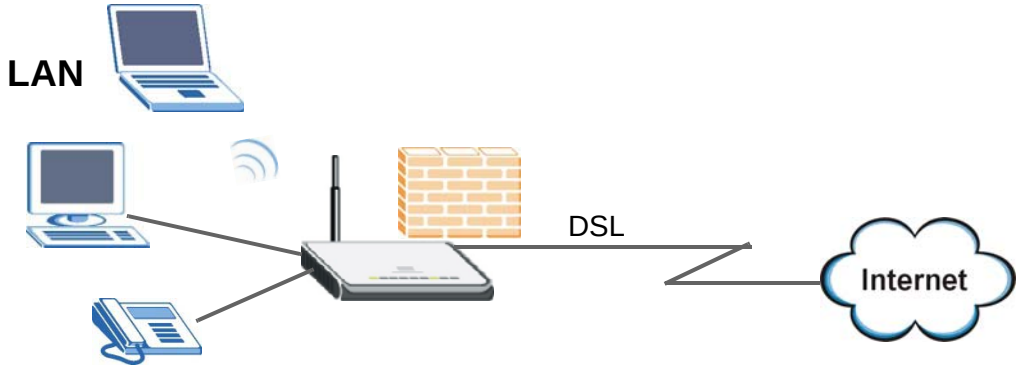
LABEL	DESCRIPTION
Enable Auto-IP-Change mode	Select this option to have the NBG4115 change its LAN IP address to 10.0.0.1 or 192.168.1.1 accordingly when the NBG4115 gets a dynamic WAN IP address in the same subnet as the LAN IP address 192.168.1.1 or 10.0.0.1. The NAT, DHCP server and firewall functions on the NBG4115 are still available in this mode.
Apply	Click **Apply** to save your changes back to the NBG4115.
Reset	Click **Reset** to begin configuring this screen afresh.

9 LAN

9.1 Overview

This chapter describes how to configure LAN settings.

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building. The LAN screens can help you configure a LAN DHCP server, manage IP addresses, and partition your physical network into logical networks.



The LAN screens can help you configure a LAN DHCP server and manage IP addresses.

9.1.1 What You Can Do in this Chapter

Use the **IP** (Section 9.3 on page 114) screen to change your basic LAN settings.

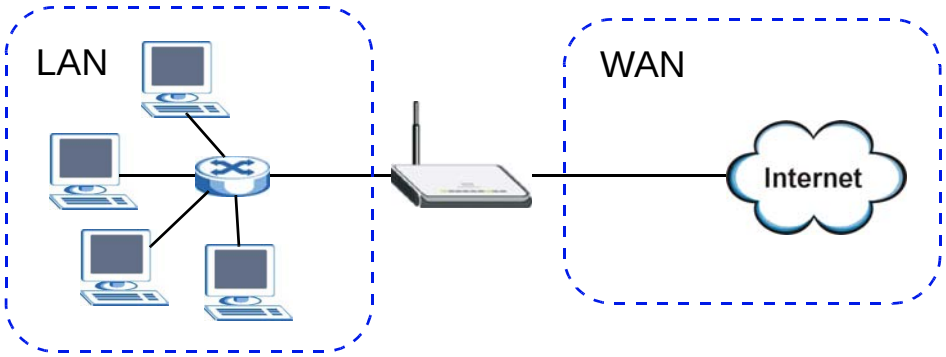
9.2 What You Need To Know

The following terms and concepts may help as you read through this chapter.

LAN and WAN IP Addresses

The actual physical connection determines whether the NBG4115 ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

Figure 67 LAN and WAN IP Addresses



The LAN parameters of the NBG4115 are preset in the factory with the following values:

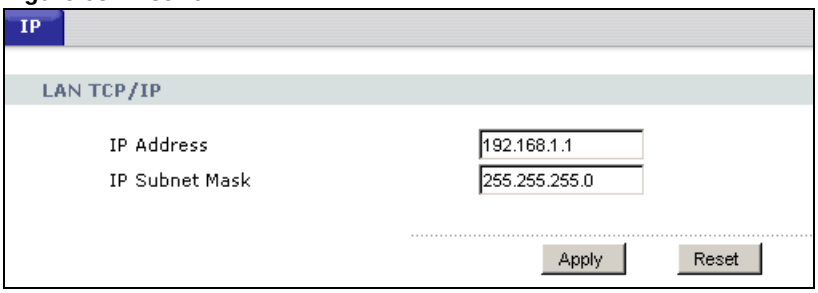
- IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits)
- DHCP server enabled with 32 client IP addresses starting from 192.168.1.33.

These parameters should work for the majority of installations. If your ISP gives you explicit DNS server address(es), read the embedded Web Configurator help regarding what fields need to be configured.

9.3 IP

Use this screen to change your basic LAN settings. Click **Network** > **LAN**.

Figure 68 Network > LAN > IP



The following table describes the labels in this screen.

Table 47 Network > LAN > IP

LABEL	DESCRIPTION
IP Address	Type the IP address of your NBG4115 in dotted decimal notation 192.168.1.1 (factory default).
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address.

Table 47 Network > LAN > IP

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the NBG4115.
Reset	Click **Reset** to begin configuring this screen afresh.

10

DHCP Server

10.1 Overview

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the NBG4115's LAN as a DHCP server or disable it. When configured as a server, the NBG4115 provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on your LAN, or else the computer must be manually configured.

10.1.1 What You Can Do in this Chapter

- Use the **General** (Section 10.2 on page 118) screen to enable the DHCP server.
- Use the **Advanced** (Section 10.3 on page 119) screen to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.
- Use the **Client List** (Section 10.4 on page 120) screen to view the current DHCP client information.

10.1.2 What You Need To Know

The following terms and concepts may help as you read through this chapter.

MAC Addresses

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. Find out the MAC addresses of your network devices if you intend to add them to the DHCP Client List screen.

Refer to Section 4.5.7 on page 51 for information on IP Address and Subnet Mask.

Refer to Section 4.5.8 on page 51 for information on System DNS Servers.

IP Pool Setup

The NBG4115 is pre-configured with a pool of 32 IP addresses starting from 192.168.1.33 to 192.168.1.64. This configuration leaves 31 IP addresses (excluding the NBG4115 itself) in the lower range (192.168.1.2 to 192.168.1.32) for other server computers, for instance, servers for mail, FTP, TFTP, web, etc., that you may have.

Refer to Section 4.5.7 on page 51 for information on IP Address and Subnet Mask.

LAN TCP/IP

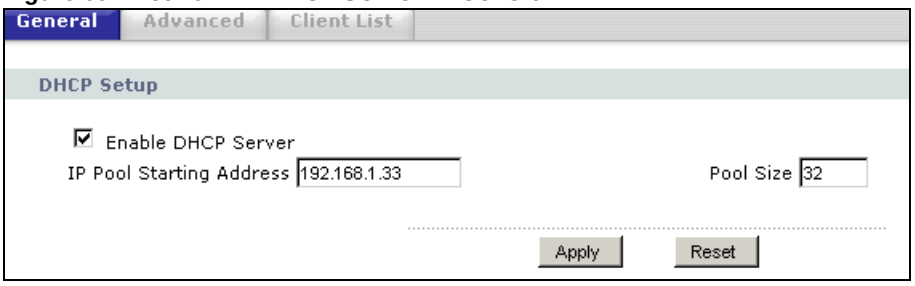
The NBG4115 has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

Refer to the Section 4.5.8 on page 51 section for information on System DNS Servers.

10.2 General

Use this screen to enable the DHCP server. Click **Network** > **DHCP Server**. The following screen displays.

Figure 69 Network > DHCP Server > General



The following table describes the labels in this screen.

Table 48 Network > DHCP Server > General

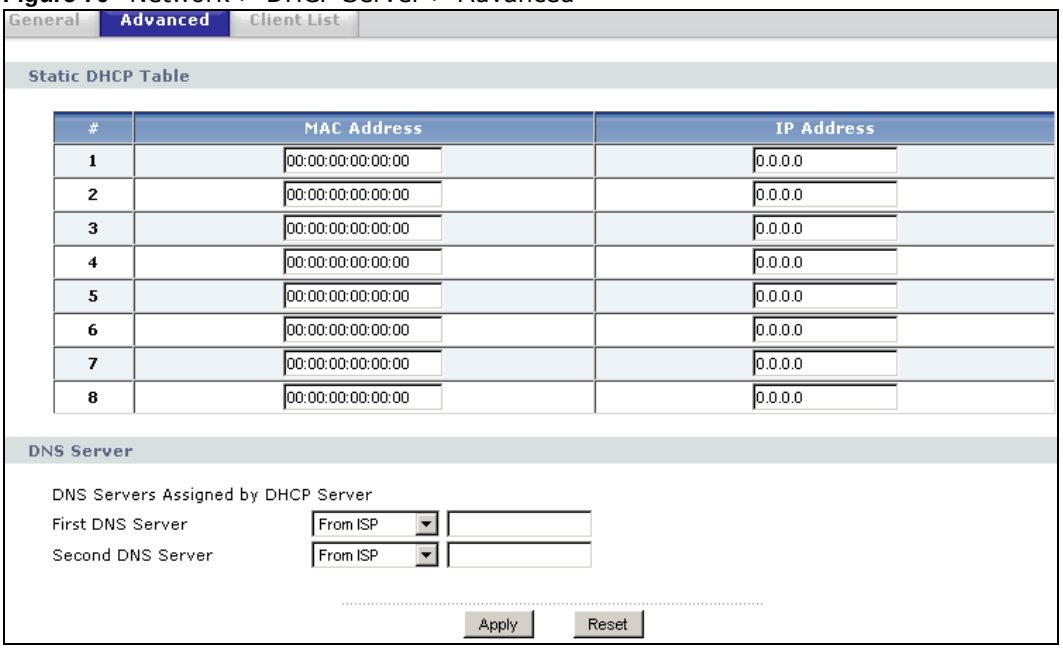
LABEL	DESCRIPTION
Enable DHCP Server	Enable or Disable DHCP for LAN. DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (computers) to obtain TCP/IP configuration at startup from a server. Leave the **Enable DHCP Server** check box selected unless your ISP instructs you to do otherwise. Clear it to disable the NBG4115 acting as a DHCP server. When configured as a server, the NBG4115 provides TCP/IP configuration for the clients. If not, DHCP service is disabled and you must have another DHCP server on your LAN, or else the computers must be manually configured. When set as a server, fill in the following four fields.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool for LAN.
Pool Size	This field specifies the size, or count of the IP address pool for LAN.
Apply	Click **Apply** to save your changes back to the NBG4115.
Reset	Click **Reset** to begin configuring this screen afresh.

10.3 Advanced

This screen allows you to assign IP addresses on the LAN to specific individual computers based on their MAC addresses. You can also use this screen to configure the DNS server information that the NBG4115 sends to the DHCP clients.

To change your NBG4115's static DHCP settings, click **Network** > **DHCP Server** > **Advanced**. The following screen displays.

Figure 70 Network > DHCP Server > Advanced



The following table describes the labels in this screen.

Table 49 Network > DHCP Server > Advanced

LABEL	DESCRIPTION
Static DHCP Table	
#	This is the index number of the static IP table entry (row).
MAC Address	Type the MAC address (with colons) of a computer on your LAN.
IP Address	Type the LAN IP address of a computer on your LAN.
DNS Server	
DNS Servers Assigned by DHCP Server	The NBG4115 passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients. The NBG4115 only passes this information to the LAN DHCP clients when you select the **Enable DHCP Server** check box. When you clear the **Enable DHCP Server** check box, DHCP service is disabled and you must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured.

Table 49 Network > DHCP Server > Advanced

LABEL	DESCRIPTION
First DNS Server Second DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the NBG4115's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **DNS Relay** to have the NBG4115 act as a DNS proxy. The NBG4115's LAN IP address displays in the field to the right (read-only). The NBG4115 tells the DHCP clients on the LAN that the NBG4115 itself is the DNS server. When a computer on the LAN sends a DNS query to the NBG4115, the NBG4115 forwards the query to the NBG4115's system DNS server (configured in the **WAN > Internet Connection** screen) and relays the response back to the computer. You can only select **DNS Relay** for one of the three servers; if you select **DNS Relay** for a second or third DNS server, that choice changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
Apply	Click **Apply** to save your changes back to the NBG4115.
Reset	Click **Reset** to begin configuring this screen afresh.

10.4 Client List

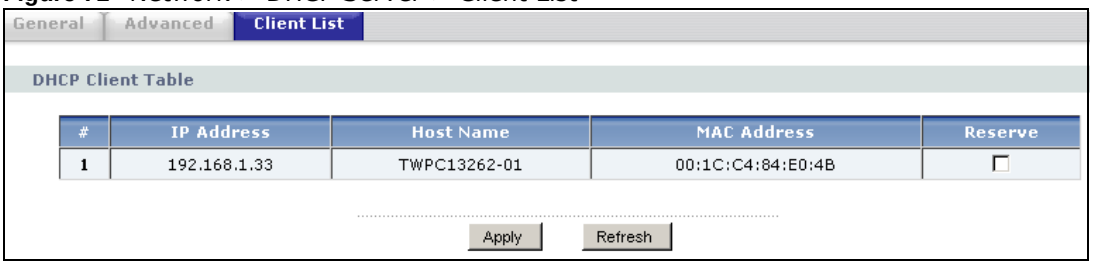
The DHCP table shows current DHCP client information (including **IP Address**, **Host Name** and **MAC Address**) of network clients using the NBG4115's DHCP servers.

Configure this screen to always assign an IP address to a MAC address (and host name). Click **Network** > **DHCP Server** > **Client List**.

Note: You can also view a read-only client list by clicking the **DHCP Table (Details...)** hyperlink in the **Status** screen.

The following screen displays.

Figure 71 Network > DHCP Server > Client List



The following table describes the labels in this screen.

Table 50 Network > DHCP Server > Client List

LABEL	DESCRIPTION
#	This is the index number of the host computer.
IP Address	This field displays the IP address relative to the # field listed above.
Host Name	This field displays the computer host name.
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
Reserve	Select this check box in the **DHCP Setup** section to have the NBG4115 always assign the IP address(es) to the MAC address(es) (and host name(s)). After you click **Apply**, the MAC address and IP address also display in the **Advanced** screen (where you can edit them).
Apply	Click **Apply** to save your settings.
Refresh	Click **Refresh** to reload the DHCP table.

11

NAT

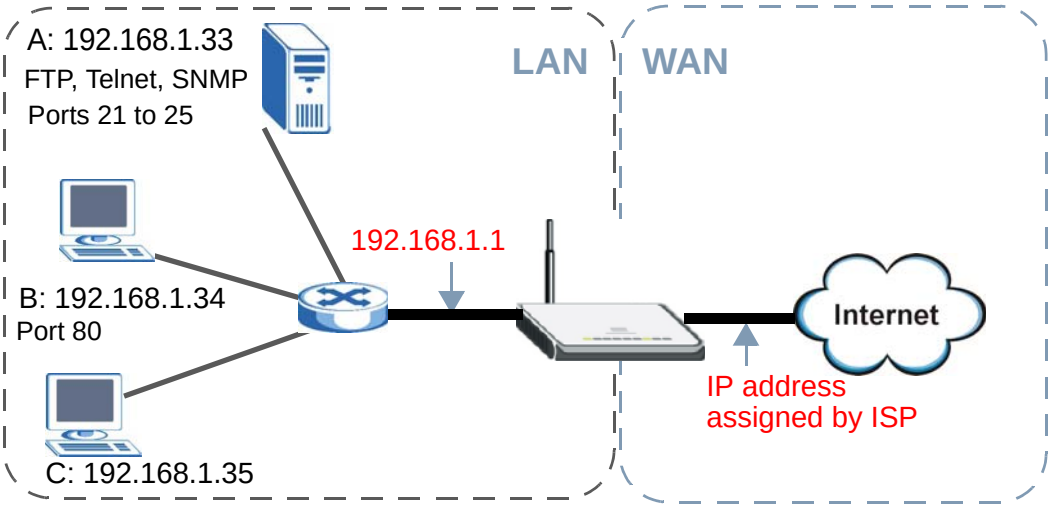
11.1 Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet. For example, the source address of an outgoing packet, used within one network is changed to a different IP address known within another network.

The figure below is a simple illustration of a NAT network. You want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example).

You assign the LAN IP addresses to the devices (**A** to **D**) connected to your NBG4115. The ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet. All traffic coming from **A** to **D** going out to the Internet use the IP address of the NBG4115, which is 192.168.1.1.

Figure 72 NAT Example



This chapter discusses how to configure NAT on the NBG4115.

Note: You must create a firewall rule in addition to setting up NAT, to allow traffic from the WAN to be forwarded through the NBG4115.

11.1.1 What You Can Do in this Chapter

- Use the **General** (Section 11.2 on page 125) screen to enable NAT and set a default server.
- Use the **Application** (Section 11.3 on page 126) screen to change your NBG4115's port forwarding settings.

- Use the **Advanced** (Section 11.5.3 on page 130) screen to change your NBG4115's trigger port settings.

11.1.2 What You Need To Know

The following terms and concepts may help as you read through this chapter.

Inside/Outside

This denotes where a host is located relative to the NBG4115, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/Local

This denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note: Inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet.

An inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 51 NAT Definitions

ITEM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

Note: NAT never changes the IP address (either local or global) of an outside host.

What NAT Does

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

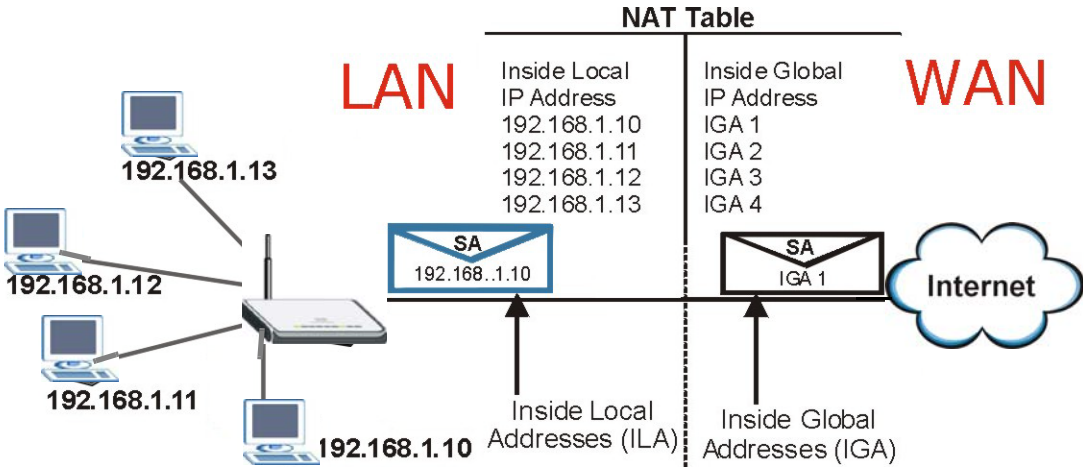
The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers , NAT offers the additional benefit of firewall protection. With no servers defined, your NBG4115 filters out

all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631, The IP Network Address Translator (NAT)*.

How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address in each packet and then forwards it to the Internet. The NBG4115 keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

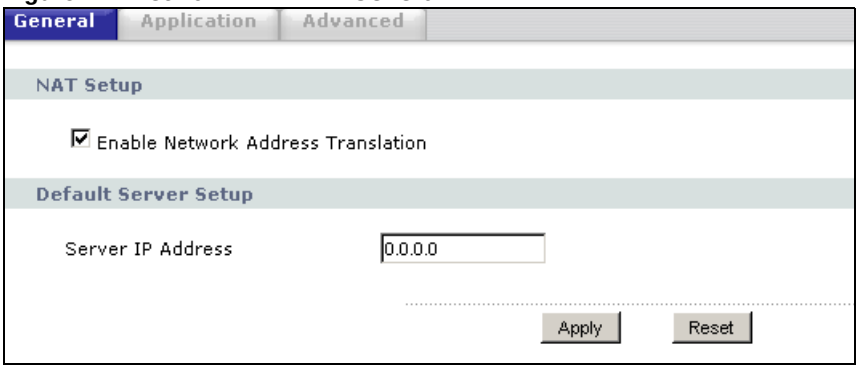
Figure 73 How NAT Works



11.2 General

Use this screen to enable NAT and set a default server. Click **Network > NAT** to open the **General** screen.

Figure 74 Network > NAT > General



The following table describes the labels in this screen.

Table 52 Network > NAT > General

LABEL	DESCRIPTION
NAT Setup	
Enable Network Address Translation	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Select the check box to enable NAT.
Default Server Setup	
Server IP Address	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in the **Application** screen. If you do not assign a **Default Server IP address**, the NBG4115 discards all packets received for ports that are not specified in the **Application** screen or remote management.
Apply	Click **Apply** to save your changes back to the NBG4115.
Reset	Click **Reset** to begin configuring this screen afresh.

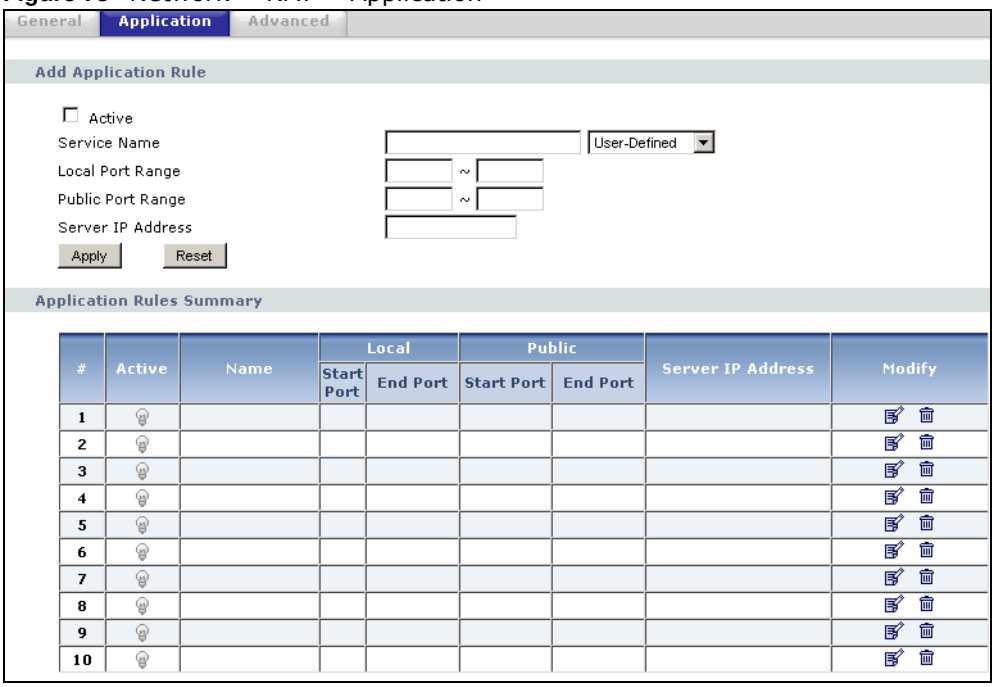
11.3 Application

Port forwarding allows you to define the local servers to which the incoming services will be forwarded. To change your NBG4115's port forwarding settings, click **Network > NAT** > **Application**. The screen appears as shown.

Note: If you do not assign a **Default Server IP address** in the **NAT > General** screen, the NBG4115 discards all packets received for ports that are not specified in this screen or remote management.

Refer to Appendix E on page 257 for port numbers commonly used for particular services.

Figure 75 Network > NAT > Application



The following table describes the labels in this screen.

Table 53 NAT Application

LABEL	DESCRIPTION
Add Application Rule	
Active	Select the check box to enable this rule and the requested service can be forwarded to the host with a specified internal IP address. Clear the checkbox to disallow forwarding of these ports to an inside server without having to delete the entry.
Service Name	Type a name (of up to 31 printable characters) to identify this rule in the first field next to **Service Name**. Otherwise, select a predefined service in the second field next to **Service Name**. The predefined service name and port number(s) will display in the **Service Name** and **Port** fields.
Local Port Range Public Port Range	Enter the start and end port(s) to be forwarded.
Server IP Address	Type the inside IP address of the server that receives packets from the port(s) specified in the **Port** field.
Apply	Click **Apply** to save your changes to the **Application Rules Summary** table.
Reset	Click **Reset** to not save and return your new changes in the **Service Name** and **Port** fields to the previous one.
Application Rules Summary	
#	This is the number of an individual port forwarding server entry.
Active	This icon is turned on when the rule is enabled.
Name	This field displays a name to identify this rule.

Table 53 NAT Application (continued)

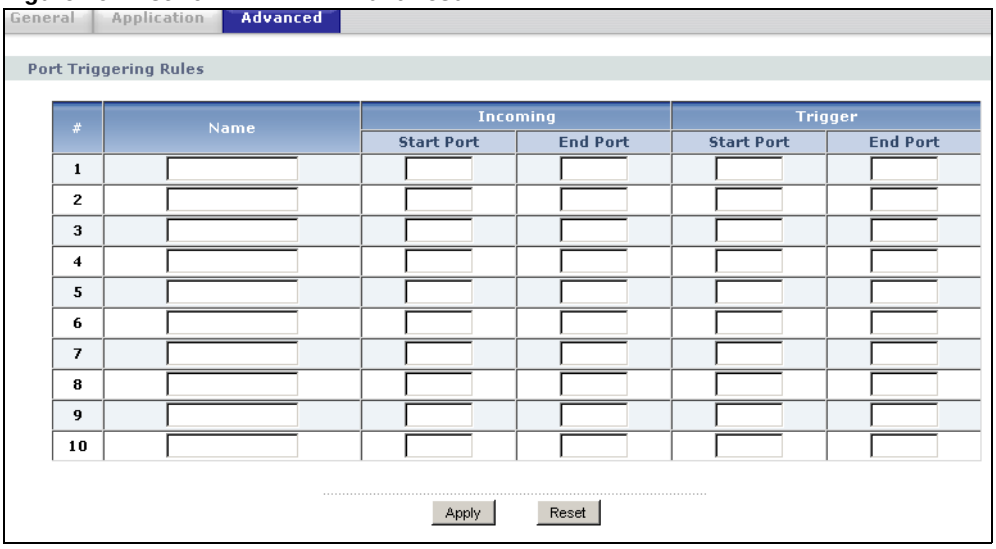
LABEL	DESCRIPTION
Local Start/End Port Public Start/End Port	This field displays the port number(s).
Server IP Address	This field displays the inside IP address of the server.
Modify	Click the **Edit** icon to display and modify an existing rule setting in the fields under **Add Application Rule**. Click the **Remove** icon to delete a rule.

11.4 Advanced

To change your NBG4115's trigger port settings, click **Network > NAT** > **Advanced**. The screen appears as shown.

Note: Only one LAN computer can use a trigger port (range) at a time.

Figure 76 Network > NAT > Advanced



The following table describes the labels in this screen.

Table 54 Network > NAT > Advanced

LABEL	DESCRIPTION
#	This is the rule index number (read-only).
Name	Type a unique name (up to 15 characters) for identification purposes. All characters are permitted - including spaces.
Incoming	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The NBG4115 forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the NBG4115 to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Apply	Click **Apply** to save your changes back to the NBG4115.
Reset	Click **Reset** to begin configuring this screen afresh.

11.5 Technical Reference

The following section contains additional technical information about the NBG4115 features described in this chapter.

11.5.1 NATPort Forwarding: Services and Port Numbers

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make accessible to the outside world even though NAT makes your whole inside network appear as a single machine to the outside world.

Use the **Application** screen to forward incoming service requests to the server(s) on your local network. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers.

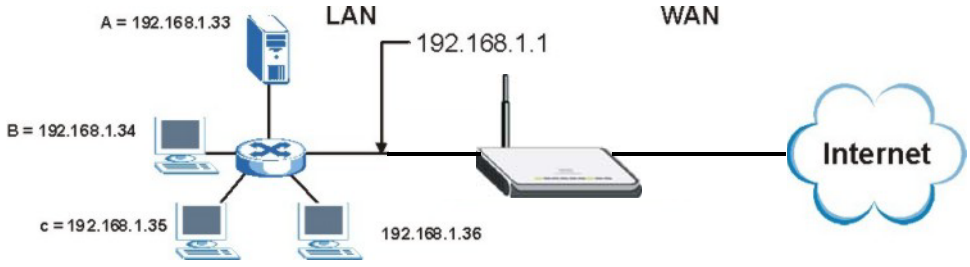
In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.

Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

11.5.2 NAT Port Forwarding Example

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 77 Multiple Servers Behind NAT Example



11.5.3 Trigger Port Forwarding

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to

use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The NBG4115 records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the NBG4115's WAN port receives a response with a specific port number and protocol ("incoming" port), the NBG4115 forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

11.5.4 Trigger Port Forwarding Example

The following is an example of trigger port forwarding.

Figure 78 Trigger Port Forwarding Process: Example

1. Jane requests a file from the Real Audio server (port 7070).
2. Port 7070 is a "trigger" port and causes the NBG4115 to record Jane's computer IP address. The NBG4115 associates Jane's computer IP address with the "incoming" port range of 6970-7170.
3. The Real Audio server responds using a port number ranging between 6970-7170.
4. The NBG4115 forwards the traffic to Jane's computer IP address.
5. Only Jane can connect to the Real Audio server until the connection is closed or times out. The NBG4115 times out in three minutes with UDP (User Datagram Protocol), or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

11.5.5 Two Points To Remember About Trigger Ports

1. Trigger events only happen on data that is going coming from inside the NBG4115 and going to the outside.
2. If an application needs a continuous data stream, that port (range) will be tied up so that another computer on the LAN can't trigger it.

12

DDNS

12.1 Overview

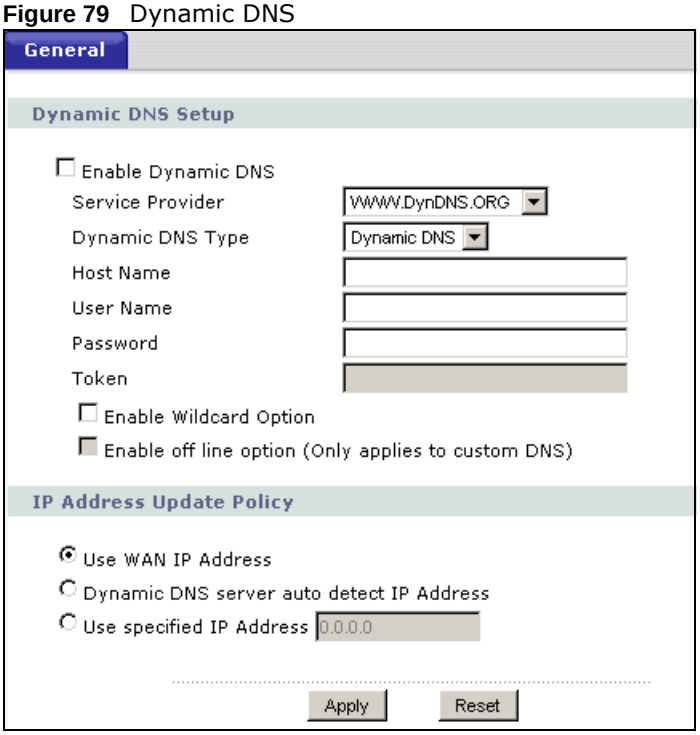
Dynamic Domain Name Service (DDNS) services let you use a fixed domain name with a dynamic IP address. Users can always use the same domain name instead of a different dynamic IP address that changes each time to connect to the NBG4115 or a server in your network.

Note: The NBG4115 must have a public global IP address and you should have your registered DDNS account information on hand.

12.2 General

To change your NBG4115's DDNS, click **Network > DDNS**. The screen appears as shown.

Figure 79 Dynamic DNS



The following table describes the labels in this screen.

Table 55 Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS Setup	
Enable Dynamic DNS	Select this check box to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
Dynamic DNS Type	This field is only available if you use the DynDNS service provider. Select the type of DNS service you are using. Use **Dynamic DNS** if you are using a dynamic IP address. Use **Static DNS** if you are hosting a server with a static IP address. Use **Custom DNS** if you want to keep hosts in your domain automatically updated with dynamic IP addresses and you want DynDNS to host its reverse DNS records.
Host Name	The host name is the domain name that the DDNS service will map to your dynamic global IP address. Type the host name fully qualified, for example, 'yourhost.mydomain.net'. You can specify up to two host names in the field separated by a comma (",").
User Name	Type the user name that you used when you registered with the DDNS service.
Password	Type the password associated with the DDNS user name.
Token	Enter your client authorization key provided by the server to update DynDNS records. This field is configurable only when you select **WWW.REGFISH.COM** in the **Service Provider** field.
Enable Wildcard Option	Select the check box to enable DynDNS Wildcard.
Enable off line option	This option is available when **CustomDNS** is selected in the **DDNS Type** field. Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
IP Address Update Policy:	
Use WAN IP Address	Select this option to update the IP address of the host name(s) to the WAN IP address.
Dynamic DNS server auto detect IP Address	Select this option to update the IP address of the host name(s) automatically by the DDNS server. It is recommended that you select this option.
Use specified IP Address	Type the IP address of the host name(s). Use this if you have a static IP address.
Apply	Click **Apply** to save your changes back to the NBG4115.
Reset	Click **Reset** to begin configuring this screen afresh.

13 Firewall

13.1 Overview

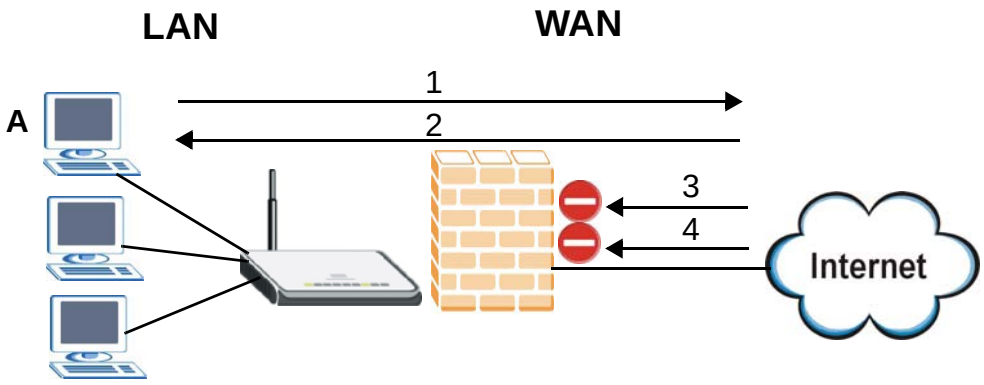
Use these screens to enable and configure the firewall that protects your NBG4115 and your LAN from unwanted or malicious traffic.

Enable the firewall to protect your LAN computers from attacks by hackers on the Internet and control access between the LAN and WAN. By default the firewall:

- allows traffic that originates from your LAN computers to go to all of the networks.
- blocks traffic that originates on the other networks from going to the LAN.

The following figure illustrates the default firewall action. User **A** can initiate an IM (Instant Messaging) session from the LAN to the WAN (1). Return traffic for this session is also allowed (2). However other traffic initiated from the WAN is blocked (3 and 4).

Figure 80 Default Firewall Action



13.1.1 What You Can Do in this Chapter

- Use the **General** screen (Section 13.2 on page 137) to enable or disable the NBG4115's firewall.
- Use the **Services** screen (Section 13.3 on page 137) screen enable service blocking, enter/delete/modify the services you want to block and the date/time you want to block them.

13.1.2 What You Need To Know

The following terms and concepts may help as you read through this chapter.

What is a Firewall?

Originally, the term “firewall” referred to a construction technique designed to prevent the spread of fire from one room to another. The networking term "firewall" is a system or group of systems that enforces an access-control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from a network that is not trusted. Of course, firewalls cannot solve every security problem. A firewall is one of the mechanisms used to establish a network security perimeter in support of a network security policy. It should never be the only mechanism or method employed. For a firewall to guard effectively, you must design and deploy it appropriately. This requires integrating the firewall into a broad information-security policy. In addition, specific policies must be implemented within the firewall itself.

Stateful Inspection Firewall

Stateful inspection firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also "inspect" the session data to assure the integrity of the connection and to adapt to dynamic protocols. These firewalls generally provide the best speed and transparency; however, they may lack the granular application level access control or caching that some proxies support. Firewalls, of one type or another, have become an integral part of standard security solutions for enterprises.

About the NBG4115 Firewall

The NBG4115’s firewall feature physically separates the LAN and the WAN and acts as a secure gateway for all data passing between the networks.

It is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated (click the **General** tab under **Firewall** and then click the **Enable Firewall** check box). The NBG4115's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The NBG4115 can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network.

The NBG4115 is installed between the LAN and a broadband modem connecting to the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

The NBG4115 has one Ethernet WAN port and four Ethernet LAN ports, which are used to physically separate the network into two areas.The WAN (Wide Area Network) port attaches to the broadband (cable or DSL) modem to the Internet.

The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP and the World Wide Web. However, "inbound access" is not allowed (by default) unless the remote host is authorized to use a specific service.

Guidelines For Enhancing Security With Your Firewall

1. Change the default password via Web Configurator.
2. Think about access control before you connect to the network in any way, including attaching a modem to the port.
3. Limit who can access your router.

4 Don't enable any local service (such as NTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.

5 For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.

6 Protect against IP spoofing by making sure the firewall is active.

7 Keep the firewall in a secured (locked) room.

13.2 General

Use this screen to enable or disable the NBG4115's firewall, and set up firewall logs. Click **Security** > **Firewall** to open the **General** screen.

Figure 81 Security > Firewall > General l

The following table describes the labels in this screen.

Table 56 Security > Firewall > General

LABEL	DESCRIPTION
Enable Firewall	Select this check box to activate the firewall. The NBG4115 performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Apply	Click **Apply** to save the settings.
Reset	Click **Reset** to start configuring this screen again.

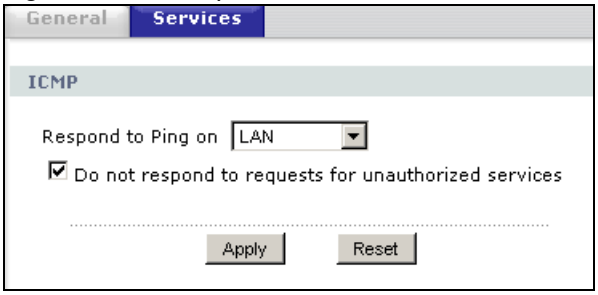
13.3 Services

If an outside user attempts to probe an unsupported port on your NBG4115, an ICMP response packet is automatically returned. This allows the outside user to know the NBG4115 exists. Use this screen to prevent the ICMP response packet from being sent. This keeps outsiders from discovering your NBG4115 when unsupported ports are probed.

You can also use this screen to enable service blocking, enter/delete/modify the services you want to block and the date/time you want to block them.

Click **Security** > **Firewall** > **Services**. The screen appears as shown next.

Figure 82 Security > Firewall > Services l



The following table describes the labels in this screen.

Table 57 Security > Firewall > Services

LABEL	DESCRIPTION
ICMP	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.
Respond to Ping on	The NBG4115 will not respond to any incoming Ping requests when **Disable** is selected. Select **LAN** to reply to incoming LAN Ping requests. Select **WAN** to reply to incoming WAN Ping requests. Otherwise select **LAN & WAN** to reply to all incoming LAN and WAN Ping requests.
Do not respond to requests for unauthorized services	Select this option to prevent hackers from finding the NBG4115 by probing for unused ports. If you select this option, the NBG4115 will not respond to port request(s) for unused ports, thus leaving the unused ports and the NBG4115 unseen. By default this option is not selected and the NBG4115 will reply with an ICMP Port Unreachable packet for a port probe on its unused UDP ports, and a TCP Reset packet for a port probe on its unused TCP ports. Note that the probing packets must first traverse the NBG4115's firewall mechanism before reaching this anti-probing mechanism. Therefore if the firewall mechanism blocks a probing packet, the NBG4115 reacts based on the firewall policy, which by default, is to send a TCP reset packet for a blocked TCP packet. You can use the command "sys firewall tcprst rst [on|off]" to change this policy. When the firewall mechanism blocks a UDP packet, it drops the packet without sending a response packet.
Apply	Click **Apply** to save the settings.
Reset	Click **Reset** to start configuring this screen again.

14

Content Filtering

14.1 Overview

This chapter provides a brief overview of content filtering using the embedded web GUI.

Internet content filtering allows you to create and enforce Internet access policies tailored to your needs. Content filtering is the ability to block certain web features or specific URL keywords.

14.1.1 What You Can Do in this Chapter

Use the **Filter** (Section 14.2 on page 140) screen to restrict web features, add keywords for blocking and designate a trusted computer.

14.1.2 What You Need To Know

The following terms and concepts may help as you read through this chapter.

Content Filtering Profiles

Content filtering allows you to block certain web features, such as cookies, and/or block access to specific web sites. For example, you can configure one policy that blocks John Doe's access to arts and entertainment web pages.

A content filtering profile conveniently stores your custom settings for the following features.

Keyword Blocking URL Checking

The NBG4115 checks the URL's domain name (or IP address) and file path separately when performing keyword blocking.

The URL's domain name or IP address is the characters that come before the first slash in the URL. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the domain name is www.zyxel.com.tw.

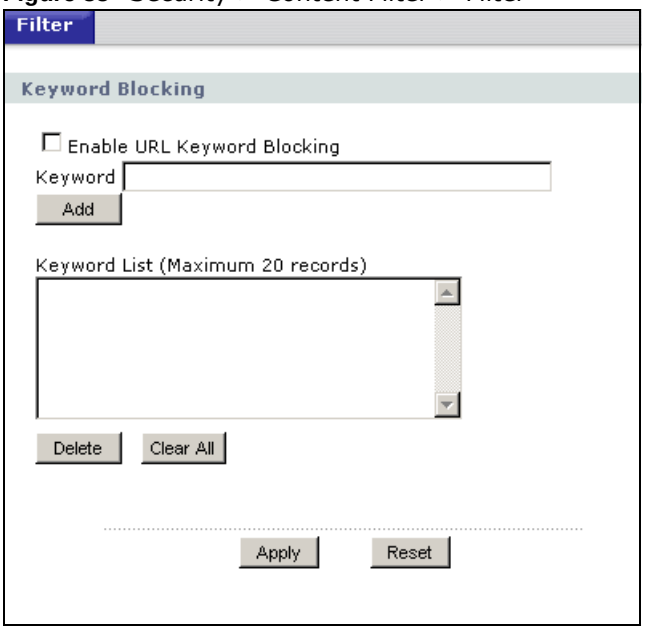
The file path is the characters that come after the first slash in the URL. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the file path is news/pressroom.php.

Since the NBG4115 checks the URL's domain name (or IP address) and file path separately, it will not find items that go across the two. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the NBG4115 would find "tw" in the domain name (www.zyxel.com.tw). It would also find "news" in the file path (news/pressroom.php) but it would not find "tw/news".

14.2 Filter

Use this screen to restrict web features, add keywords for blocking and designate a trusted computer. Click **Security** > **Content Filter** to open the **Filter** screen.

Figure 83 Security > Content Filter > Filter



The following table describes the labels in this screen.

Table 58 Security > Content Filter > Filter

LABEL	DESCRIPTION
Enable URL Keyword Blocking	The NBG4115 can block Web sites with URLs that contain certain keywords in the domain name or IP address. For example, if the keyword "bad" was enabled, all sites containing this keyword in the domain name or IP address will be blocked, e.g., URL http://www.website.com/bad.html would be blocked. Select this check box to enable this feature.
Keyword	Type a keyword in this field. You may use any character (up to 64 characters). Wildcards are not allowed. You can also enter a numerical IP address.
Keyword List	This list displays the keywords already added.
Add	Click **Add** after you have typed a keyword. Repeat this procedure to add other keywords. Up to 64 keywords are allowed. When you try to access a web page containing a keyword, you will get a message telling you that the content filter is blocking this request.
Delete	Highlight a keyword in the lower box and click **Delete** to remove it. The keyword disappears from the text box after you click **Apply**.
Clear All	Click this button to remove all of the listed keywords.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh

14.3 Technical Reference

The following section contains additional technical information about the NBG4115 features described in this chapter.

14.3.1 Customizing Keyword Blocking URL Checking

You can use commands to set how much of a website's URL the content filter is to check for keyword blocking. See the appendices for information on how to access and use the command interpreter.

Domain Name or IP Address URL Checking

By default, the NBG4115 checks the URL's domain name or IP address when performing keyword blocking.

This means that the NBG4115 checks the characters that come before the first slash in the URL.

For example, with the URL www.zyxel.com.tw/news/pressroom.php, content filtering only searches for keywords within www.zyxel.com.tw.

Full Path URL Checking

Full path URL checking has the NBG4115 check the characters that come before the last slash in the URL.

For example, with the URL www.zyxel.com.tw/news/pressroom.php, full path URL checking searches for keywords within www.zyxel.com.tw/news/.

Use the `ip urlfilter customize actionFlags 6 [disable | enable]` command to extend (or not extend) the keyword blocking search to include the URL's full path.

File Name URL Checking

Filename URL checking has the NBG4115 check all of the characters in the URL.

For example, filename URL checking searches for keywords within the URL www.zyxel.com.tw/news/pressroom.php.

Use the `ip urlfilter customize actionFlags 8 [disable | enable]` command to extend (or not extend) the keyword blocking search to include the URL's complete filename.

15

Static Route

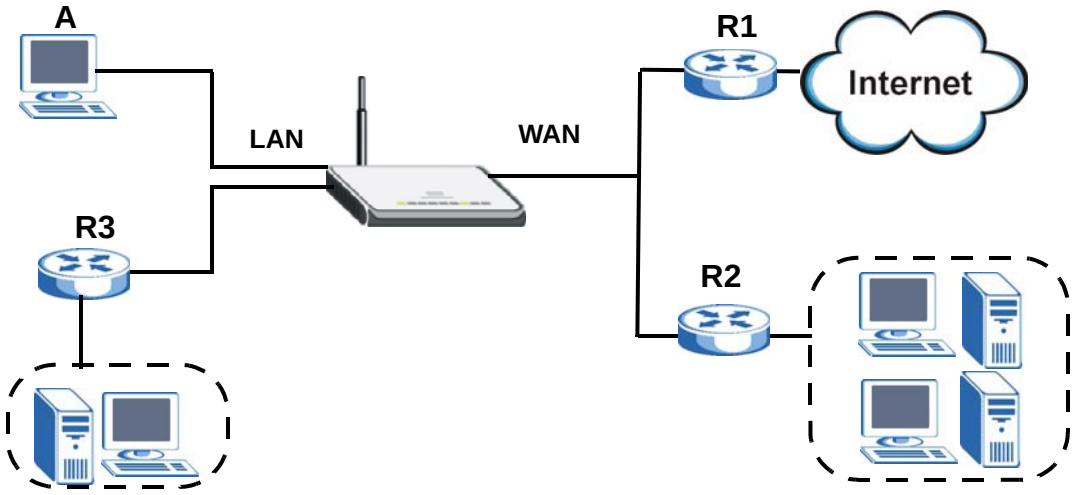
15.1 Overview

This chapter shows you how to configure static routes for your NBG4115.

The NBG4115 usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the NBG4115 send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the NBG4115's LAN interface. The NBG4115 routes most traffic from **A** to the Internet through the NBG4115's default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate network behind a router **R3** connected to the LAN.

Figure 84 Example of Static Routing Topology



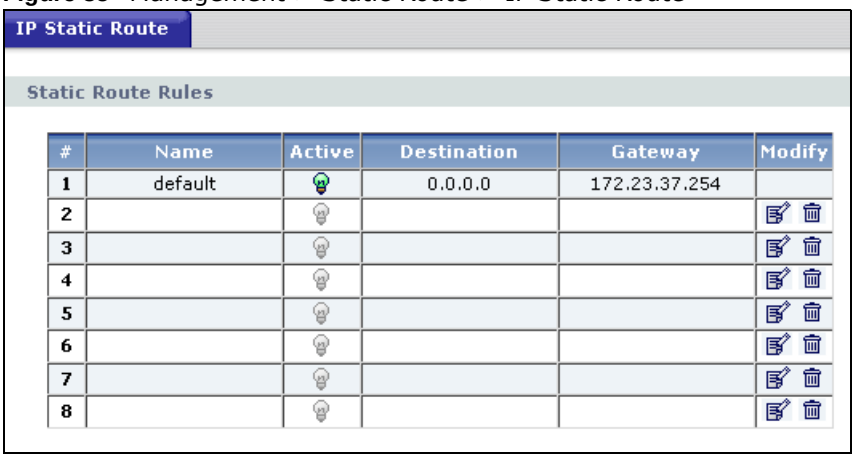
15.1.1 What You Can Do in this Chapter

- Use the **IP Static Route** screen (Section 15.2 on page 144) to view existing static route rules.
- Use the **Static Route Setup** screen (Section 15.2.1 on page 145) to add or edit a static route rule.

15.2 IP Static Route

Use this screen to view existing static route rules. Click **Management** > **Static Route** to open the **IP Static Route** screen. The following screen displays.

Figure 85 Management > Static Route > IP Static Route



The following table describes the labels in this screen.

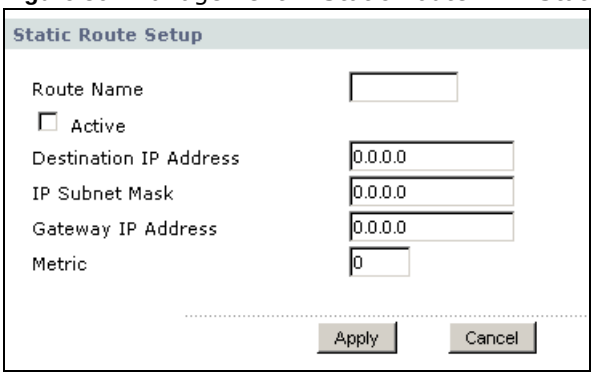
Table 59 Management > Static Route > IP Static Route

LABEL	DESCRIPTION
#	This is the index number of an individual static route. The first entry is for the default route and not editable.
Name	This is the name that describes or identifies this route.
Active	This icon is turned on when this static route is active. Click the **Edit** icon under **Modify** and select the **Active** checkbox in the **Static Route Setup** screen to enable the static route. Clear the checkbox to disable this static route without having to delete the entry.
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Gateway	This is the IP address of the gateway. The gateway is an immediate neighbor of your NBG4115 that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your NBG4115; over the WAN, the gateway must be the IP address of one of the remote nodes.
Modify	Click the **Edit** icon to open the static route setup screen. Modify a static route or create a new static route in the **Static Route Setup** screen. Click the **Remove** icon to delete a static route.

15.2.1 Static Route Setup Screen

To edit a static route, click the edit icon under **Modify**. The following screen displays. Fill in the required information for each static route.

Figure 86 Management > Static Route > IP Static Route: Static Route Setup



The following table describes the labels in this screen.

Table 60 Management > Static Route > IP Static Route: Static Route Setup

LABEL	DESCRIPTION
Route Name	Enter the name of the IP static route. Leave this field blank to delete this static route.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your NBG4115 that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your NBG4115; over the WAN, the gateway must be the IP address of one of the Remote Nodes.
Metric	Metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Apply	Click **Apply** to save your changes back to the NBG4115.
Cancel	Click **Cancel** to return to the previous screen and not save your changes.

16

Bandwidth Management

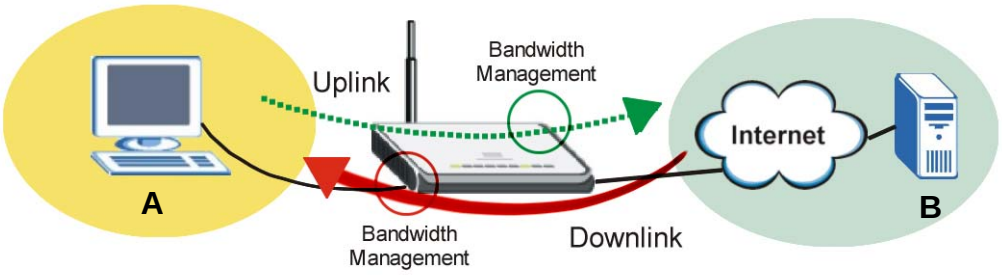
16.1 Overview

This chapter contains information about configuring bandwidth management and editing rules.

ZyXEL's Bandwidth Management allows you to specify bandwidth management rules based on an application.

In the figure below, uplink traffic goes from the LAN device (**A**) to the WAN device (**B**). Bandwidth management is applied before sending the packets out to the WAN. Downlink traffic comes back from the WAN device (**B**) to the LAN device (**A**). Bandwidth management is applied before sending the traffic out to LAN.

Figure 87 Bandwidth Management



You can allocate specific amounts of bandwidth capacity (bandwidth budgets) to individual applications (like VoIP, Web, FTP, and E-mail for example).

16.1.1 What You Can Do in this Chapter

- Use the **General** screen (Section 16.2 on page 147) to enable bandwidth management and assign uplink/downlink limits.
- Use the **Advanced** screen (Section 16.3 on page 148) to configure bandwidth management rules for the pre-defined services and applications.

16.1.2 What You Need To Know

The following terms and concepts may help as you read through this chapter.

Bandwidth Limiting

You can limit an application's uplink or downlink bandwidth. This limit keeps the traffic from using up too much of the out-going interface's bandwidth. This way you can make sure there is bandwidth for other applications. Use the following guidelines:

- The sum of the bandwidth allotments that apply to the WAN interface (LAN to WAN, WLAN to WAN) must be less than or equal to the **Uplink** value that you configure in the **Bandwidth Management General** screen.
- The sum of the bandwidth allotments that apply to the LAN port (WAN to LAN, WAN to WLAN) must be less than or equal to the **Downlink** value that you configure in the **Bandwidth Management General** screen.

16.2 General

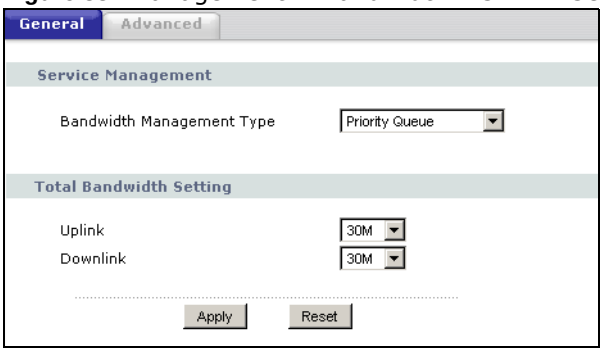
Use this screen to enable bandwidth management and assign uplink/downlink limits. You can use either one of the following types:

- **Priority Queue**. Enable bandwidth management to give uplink traffic that matches a bandwidth rule priority over traffic that does not match a bandwidth rule. (This type does not apply to downlink traffic.)
- **Bandwidth Allocation**. Enabling bandwidth management also allows you to control the maximum or minimum amounts of bandwidth that can be used by traffic that matches a bandwidth rule.

Note: You cannot apply both bandwidth management types at the same time.

Click **Management > Bandwidth MGMT** to open the bandwidth management **General** screen.

Figure 88 Management > Bandwidth MGMT > General



The following table describes the labels in this screen.

Table 61 Management > Bandwidth MGMT > General

LABEL	DESCRIPTION
Service Management	
Bandwidth Management Type	This field allows you to have NBG4115 apply bandwidth management. Select **Priority Queue** or **Bandwidth Allocation** to enable bandwidth management. Select **Priority Queue** to allocate bandwidth based on the pre-defined priority assigned to an application. Refer to Section 16.3 on page 148. Select **Bandwidth Allocation** allocate specific amounts of bandwidth to specific protocols on an IP or IP range. Refer to Section 16.3 on page 148. Select **Disable** if you do not want to use this feature.
Total Bandwidth Setting. The fields below appear when you enable Bandwidth Management.	

Table 61 Management > Bandwidth MGMT > General

LABEL	DESCRIPTION
Uplink	Select the total amount of bandwidth (from 64 Kilobits to 30 Megabits) that you want to dedicate to uplink traffic. This is traffic from LAN/WLAN to WAN.
Downlink	Select the total amount of bandwidth (from 64 Kilobits to 30 Megabits) that you want to dedicate to uplink traffic. This is traffic from WAN to LAN/WLAN.
Apply	Click **Apply** to save your customized settings.
Reset	Click **Reset** to begin configuring this screen afresh.

16.3 Advanced

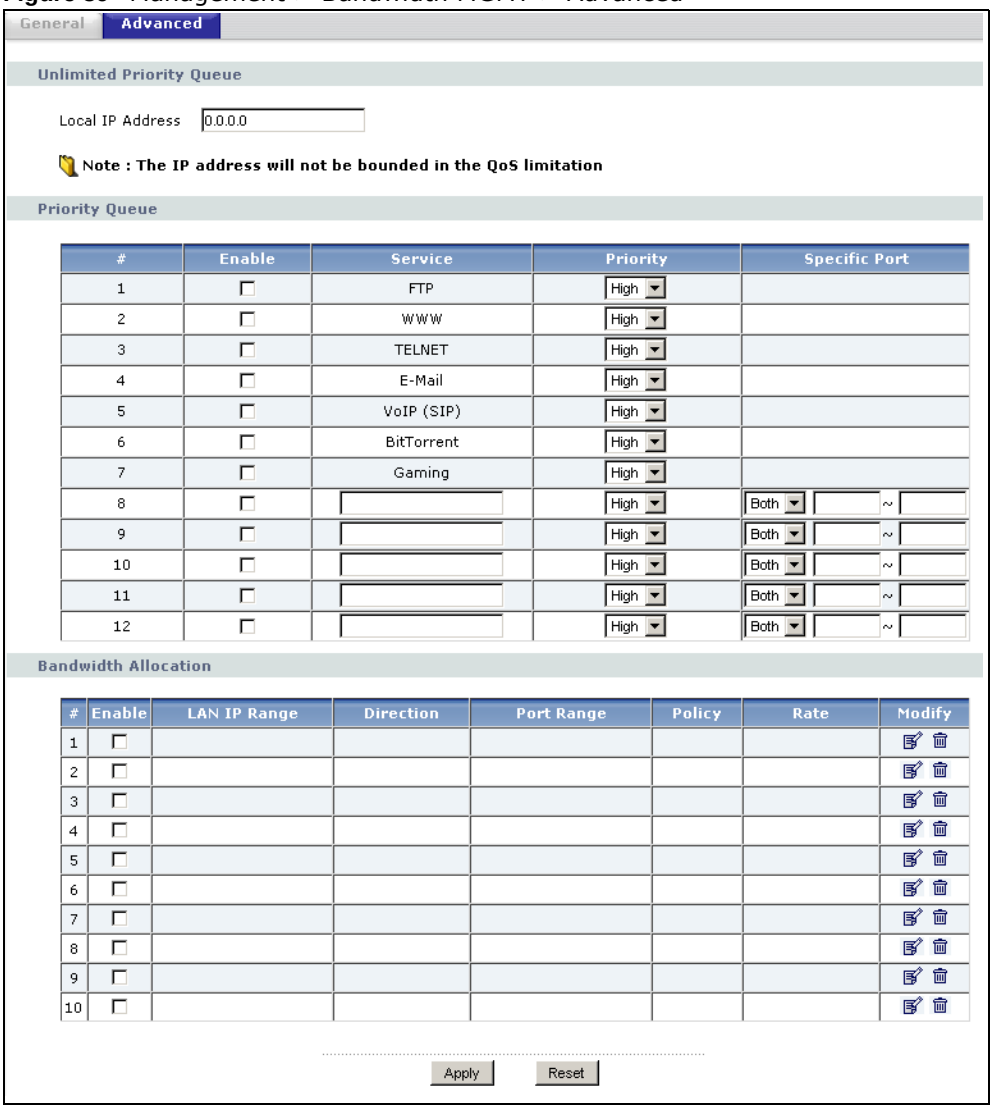
Use this screen to configure bandwidth managements rule for the pre-defined services or applications.

Use this screen to configure bandwidth managements rule for specific protocols on an IP or IP range.

Note: This screen contains the **Priority Queue** and **Bandwidth Allocation** tables. Though both tables are described in this section, you can only apply the rules in one table. Fill out the table of the **Bandwidth Management Type** you selected in Section 16.2 on page 147

Click **Management** > **Bandwidth MGMT** > **Advanced** to open the bandwidth management **Advanced** screen.

Figure 89 Management > Bandwidth MGMT > Advanced



The following table describes the labels in this screen.

Table 62 Management > Bandwidth MGMT > Advanced

LABEL	DESCRIPTION
Priority Queue	
Local IP Address	Enter the IP address of the computer to which bandwidth management does not apply.
Priority Queue	Use this table to allocate specific amounts of bandwidth based on the pre-defined service.
#	This is the number of an individual bandwidth management rule.
Enable	Select this check box to have the NBG4115 apply this bandwidth management rule.

Table 62 Management > Bandwidth MGMT > Advanced (continued)

LABEL	DESCRIPTION
Service	This is the name of the service. You can also enter the name (up to 10 keyboard characters) of a service you want to add in the priority queue (for example, **Messenger**).
Priority	Select a priority from the drop down list box. Choose **High** or **Low**.
Specific Port	This displays the port/s assigned to the service. You can also specify the port/s to services to which you want to allocate bandwidth. Choose either **Both**, **TCP** or **UDP** in the drop-down menu and enter the port or range of ports in the provided boxes. Note: If you are entering a specific port and not a range of ports, you can either leave the second port field blank or enter the same port number again.
Bandwidth Allocation	Use this table to allocate specific amounts of bandwidth to specific protocols on an IP or IP range.
#	This is the number of an individual bandwidth management rule.
Enable	Select this check box to have the NBG4115 apply this bandwidth management rule.
LAN IP Range	This displays the range of IP addresses for which the bandwidth management rule applies.
Direction	These read-only labels represent uplink or downlink traffic. **To LAN** applies bandwidth management to traffic from WAN to LAN/WLAN (i.e., downlink). **To WAN** applies bandwidth management to traffic from LAN/WLAN to WAN (i.e., uplink). **Both** applies bandwidth management to traffic that the NBG4115 forwards to both the LAN and the WAN.
Port Range	This displays the range of ports for which the bandwidth management rule applies.
Policy	This displays either **Max** (maximum) or **Min** (minimum) and refers to the maximum or minimum bandwidth allowed for the rule in kilobits per second in the field below.
Rate	This is the maximum or minimum bandwidth allowed (refer to the field above) for the rule in bits per second.
Modify	Click the **Edit** icon to open the **Rule Configuration** screen. Modify an existing rule or create a new rule in the **Rule Configuration** screen. See Section 16.3.3 on page 151 for more information. Click the **Remove** icon to delete a rule.
Apply	Click **Apply** to save your customized settings.
Reset	Click **Reset** to begin configuring this screen afresh.

16.3.1 Pre-Configured Gaming Ports

The following gaming ports are preconfigured on your NBG4115 and are enabled when you select the 'gaming' **Service** in this screen:

Table 63 Preconfigured Gaming Ports

APPLICATION	TCP PORTS	UDP PORTS
XBox 360	3074, 3390, 3932, 5555	1900, 3776, 7777, 88, 3074
Playstation	80, 443, 5223, 5223	3478, 3479, 3658, 4658
Battlenet	40, 6112, 4000, 6113- 6119, 112	
MSN Game Zone	6667, 28800-29000	6667, 28800-29000

16.3.2 Priority Levels

Traffic with a higher priority gets through faster while traffic with a lower priority is dropped if the network is congested.

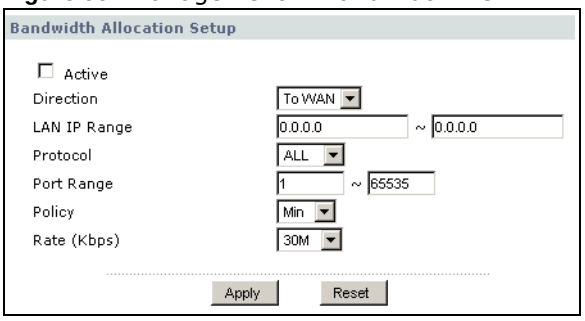
The following describes the priorities that you can apply to traffic that the NBG4115 forwards out through an interface.

- **High** - Typically used for voice traffic or video that is especially sensitive to jitter (jitter is the variations in delay).
- **Low** - This is typically used for all other traffic that are not time-sensitive.

16.3.3 User Defined Service Rule Configuration

If you want to edit a bandwidth management rule for specific protocols on an IP or IP range, click the **Edit** icon in the **Bandwidth Allocation** table of the **Advanced** screen. The following screen displays.

Figure 90 Management > Bandwidth MGMT > Advanced: Allocation Setup



The following table describes the labels in this screen.

Table 64 Management > Bandwidth MGMT > Advanced: Allocation Setup

LABEL	DESCRIPTION
Active	Select this check box to turn on this bandwidth management rule.
Direction	Enter whether you want to apply the rule to uplink or downlink traffic. **To LAN** applies bandwidth management to traffic from WAN to LAN/WLAN (i.e., downlink). **To WAN** applies bandwidth management to traffic from LAN/WLAN to WAN (i.e., uplink). Select **Both** applies bandwidth management to traffic that the NBG4115 forwards to both the LAN and the WAN.
LAN IP Range	Specify the range of IP addresses for which the bandwidth management rule applies.
Protocol	Select the protocol (**TCP**, **UDP**, **SMTP**, **HTTP**, **POP3**, **FTP** or **ALL**) for which the bandwidth management rule applies.
Port Range	Enter the range of ports for which the bandwidth management rule applies.
Policy	Select **Max** or **Min** and specify the maximum or minimum bandwidth allowed for the rule in bits per second in the field below.
Rate (bps)	Select the maximum or minimum bandwidth allowed (refer to the field above) for the rule in bits per second.
Apply	Click **Apply** to save your customized settings.
Reset	Click **Reset** to begin configuring this screen afresh.

16.3.4 Predefined Bandwidth Management Services

The following is a description of the services that you can select and to which you can apply media bandwidth management in the **Management** > **Bandwidth MGMT** > **Advanced** screen.

Table 65 Media Bandwidth Management Setup: Services

SERVICE	DESCRIPTION
FTP	File Transfer Program enables fast transfer of files, including large files that may not be possible by e-mail. FTP uses port number 21.
WWW	The World Wide Web (WWW) is an Internet system to distribute graphical, hyper-linked information, based on Hyper Text Transfer Protocol (HTTP) - a client/server protocol for the World Wide Web. The Web is not synonymous with the Internet; rather, it is just one service on the Internet. Other services on the Internet include Internet Relay Chat and Newsgroups. The Web is accessed through use of a browser. WWW uses port 80.
Telnet	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems. Telnet uses port 23.
E-Mail	Electronic mail consists of messages sent through a computer network to specific groups or individuals. Here are some default ports for e-mail: POP3 - port 110 SMTP - port 25

Table 65 Media Bandwidth Management Setup: Services (continued)

SERVICE	DESCRIPTION
VoIP (SIP)	Sending voice signals over the Internet is called Voice over IP or VoIP. Session Initiated Protocol (SIP) is an internationally recognized standard for implementing VoIP. SIP is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet. SIP is transported primarily over UDP but can also be transported over TCP, using the default port number 5060.
BitTorrent	BitTorrent is a free P2P (peer-to-peer) sharing tool allowing you to distribute large software and media files using ports 6881 to 6889. BitTorrent requires you to search for a file with a searching engine yourself. It distributes files by corporation and trading, that is, the client downloads the file in small pieces and share the pieces with other peers to get other half of the file.
Gaming	Online gaming services lets you play multiplayer games on the Internet via broadband technology. One example is Microsoft's Xbox Live, which uses port 3074. As of this writing, your NBG4115 supports Xbox, Playstation, Battlenet and MSN Game Zone.

16.3.5 Services and Port Numbers

See Appendix E on page 257 for commonly used services and port numbers.

17

Remote Management

17.1 Overview

This chapter provides information on the Remote Management screens.

Remote management allows you to determine which services/protocols can access which NBG4115 interface (if any) from which computers.

You may manage your NBG4115 from a remote location via:

- LAN only
- LAN and WAN

17.1.1 What You Can Do in this Chapter

Use the **WWW** screen (Section 17.2 on page 155) to change your NBG4115's World Wide Web settings.

17.1.2 What You Need To Know

The following terms and concepts may help as you read through this chapter.

Remote Management Limitations

Remote management over LAN or WAN will not work when:

1. You have disabled that service in one of the remote management screens.
2. The IP address in the **Secured Client IP Address** field does not match the client IP address. If it does not match, the NBG4115 will disconnect the session immediately.
3. There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.
4. There is a firewall rule that blocks it.

Remote Management and NAT

When NAT is enabled:

- Use the NBG4115's WAN IP address when configuring from the WAN.
- Use the NBG4115's LAN IP address when configuring from the LAN.

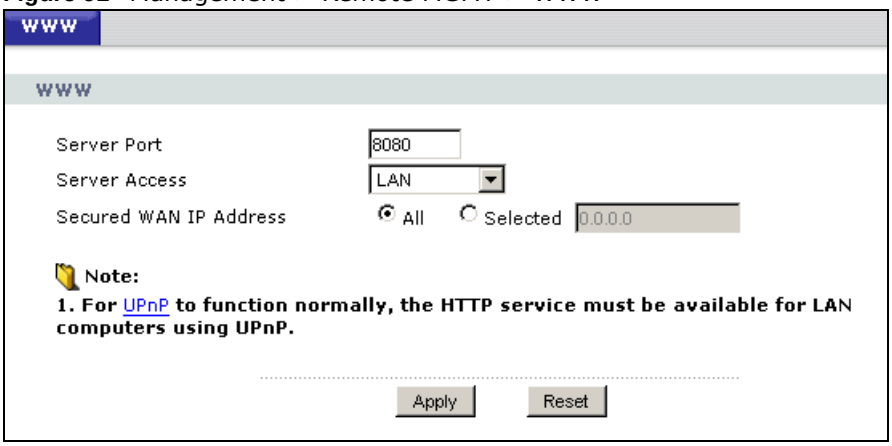
System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The NBG4115 automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling. You can change the timeout period in the **System** screen

17.2 WWW

To change your NBG4115's World Wide Web settings, click **Management** > **Remote MGMT** to display the **WWW** screen.

Figure 91 Management > Remote MGMT > WWW



The following table describes the labels in this screen.

Table 66 Management > Remote MGMT > WWW

LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the NBG4115 using this service.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the NBG4115 using this service. Select **All** to allow any computer to access the NBG4115 using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the NBG4115 using this service. Note: This only applies on WAN IP.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

18

UPnP

18.1 Overview

This chapter introduces the UPnP feature in the Web Configurator.

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

18.1.1 What You Can Do in this Chapter

Use the **UPnP** screen (Section 18.2 on page 157) to enable UPnP on the NBG4115.

18.1.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

How do I know if I'm using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See the NAT chapter for more information on NAT.

Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

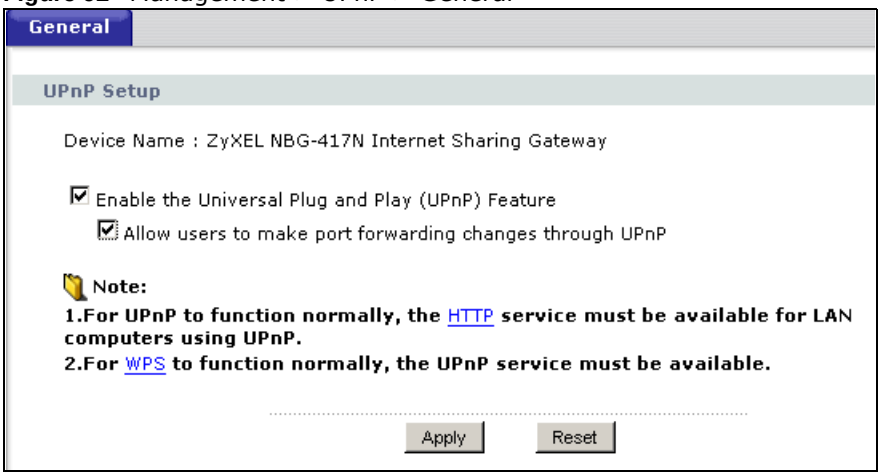
When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the NBG4115 allows multicast messages on the LAN only.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

18.2 General

Use this screen to enable UPnP. Click the **Management > UPnP** to open the following screen.

Figure 92 Management > UPnP > General


General
UPnP Setup
Device Name : ZyXEL NBG-417N Internet Sharing Gateway
Enable the Universal Plug and Play (UPnP) Feature
Allow users to make port forwarding changes through UPnP
Note:
1.For UPnP to function normally, the HTTP service must be available for LAN computers using UPnP.
2.For WPS to function normally, the UPnP service must be available.
Apply
Reset

The following table describes the labels in this screen.

Table 67 Management > UPnP > General

LABEL	DESCRIPTION
Enable the Universal Plug and Play (UPnP) Feature	Select this check box to activate UPnP. Be aware that anyone could use a UPnP application to open the Web Configurator's login screen without entering the NBG4115's IP address (although you must still enter the password to access the Web Configurator).
Allow users to make port forwarding changes through UPnP	Select this check box to allow UPnP-enabled applications to automatically configure the NBG4115 so that they can communicate through the NBG4115, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.
Apply	Click **Apply** to save the setting to the NBG4115.
Reset	Click **Reset** to begin configuring this screen afresh.

18.3 Technical Reference

The following section contains additional technical information about the NBG4115 features described in this chapter.

18.3.1 Installing UPnP in Windows XP

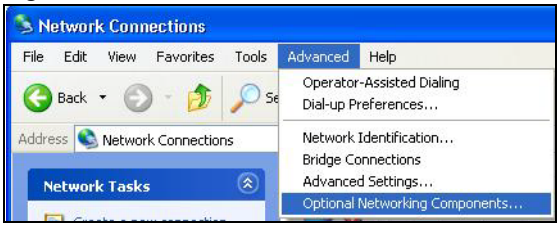
Follow the steps below to install the UPnP in Windows XP.

1 Click **Start** and **Control Panel**.

2 Double-click **Network Connections**.

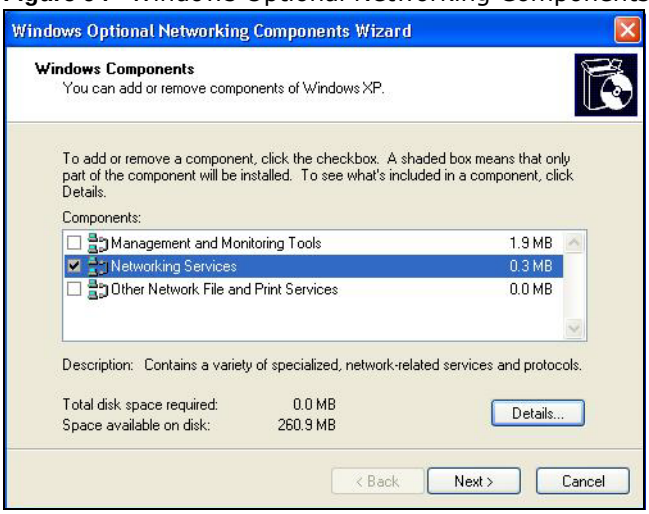
3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ...**.

Figure 93 Network Connections



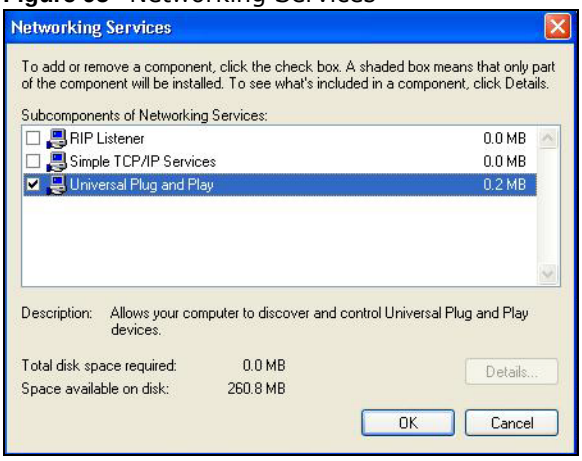
4 The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.

Figure 94 Windows Optional Networking Components Wizard


Windows Optional Networking Components Wizard
Windows Components
You can add or remove components of Windows XP.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Management and Monitoring Tools 1.9 MB
Networking Services 0.3 MB
Other Network File and Print Services 0.0 MB
Description: Contains a variety of specialized, network-related services and protocols.
Total disk space required: 0.0 MB
Space available on disk: 260.9 MB
Details...
< Back
Next >
Cancel

5 In the **Networking Services** window, select the **Universal Plug and Play** check box.

Figure 95 Networking Services


Networking Services
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Networking Services:
RIP Listener 0.0 MB
Simple TCP/IP Services 0.0 MB
Universal Plug and Play 0.2 MB
Description: Allows your computer to discover and control Universal Plug and Play devices.
Total disk space required: 0.0 MB
Space available on disk: 260.8 MB
Details...
OK
Cancel

6 Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.

18.3.1.1 Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the NBG4115.

Make sure the computer is connected to a LAN port of the NBG4115. Turn on your computer and the NBG4115.

Auto-discover Your UPnP-enabled Network Device

1 Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.

2 Right-click the icon and select **Properties**.

Figure 96 Network Connections

3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

Figure 97 Internet Connection Properties

Internet Connection Properties
General
Connect to the Internet using:
Internet Connection
This connection allows you to connect to the Internet through a shared connection on another computer.
Settings...
Show icon in notification area when connected
OK
Cancel

4 You may edit or delete the port mappings or click **Add** to manually add port mappings.

Figure 98 Internet Connection Properties: Advanced Settings

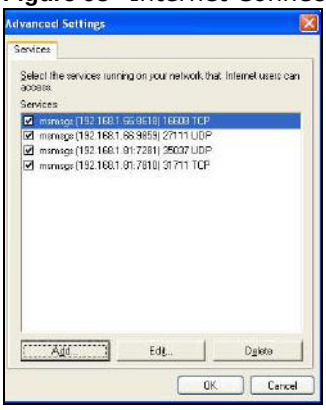
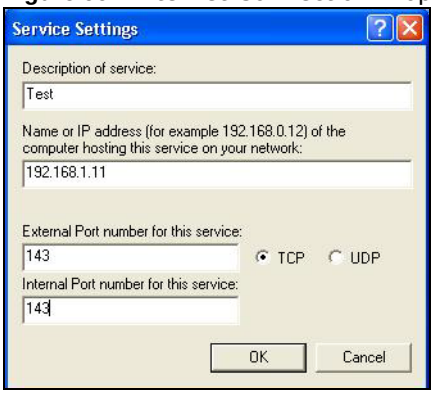


Figure 99 Internet Connection Properties: Advanced Settings: Add



5 When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

6 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.

Figure 100 System Tray Icon

7 Double-click on the icon to display your current Internet connection status.

Figure 101 Internet Connection Status

Web Configurator Easy Access

With UPnP, you can access the web-based configurator on the NBG4115 without finding out the IP address of the NBG4115 first. This comes helpful if you do not know the IP address of the NBG4115.

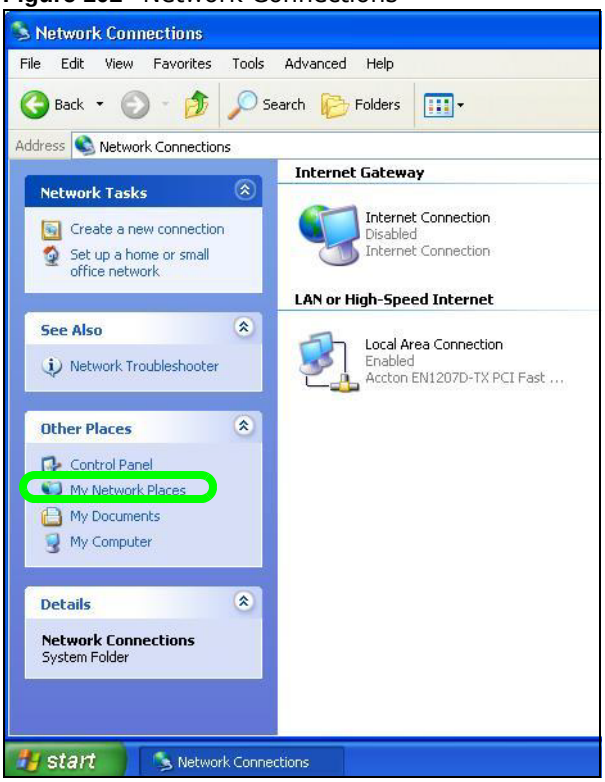
Follow the steps below to access the Web Configurator.

1 Click **Start** and then **Control Panel**.

2 Double-click **Network Connections**.

3 Select **My Network Places** under **Other Places**.

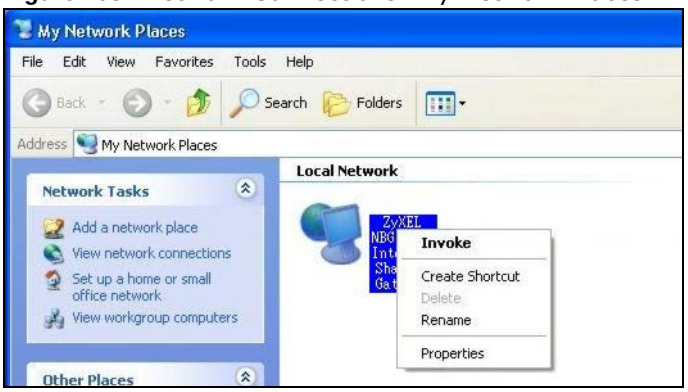
Figure 102 Network Connections



4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

5 Right-click on the icon for your NBG4115 and select **Invoke**. The Web Configurator login screen displays.

Figure 103 Network Connections: My Network Places



6 Right-click on the icon for your NBG4115 and select **Properties**. A properties window displays with basic information about the NBG4115.

Figure 104 Network Connections: My Network Places: Properties: Example

19 WoL

19.1 Overview

Wake On LAN (WoL) allows you to remotely turn on a device on the network, such as a computer, storage device or media server. To use this feature the remote hardware (for example the network adapter on a computer) must support Wake On LAN using the "Magic Packet" method.

You need to know the MAC address of the remote device. It may be on a label on the device.

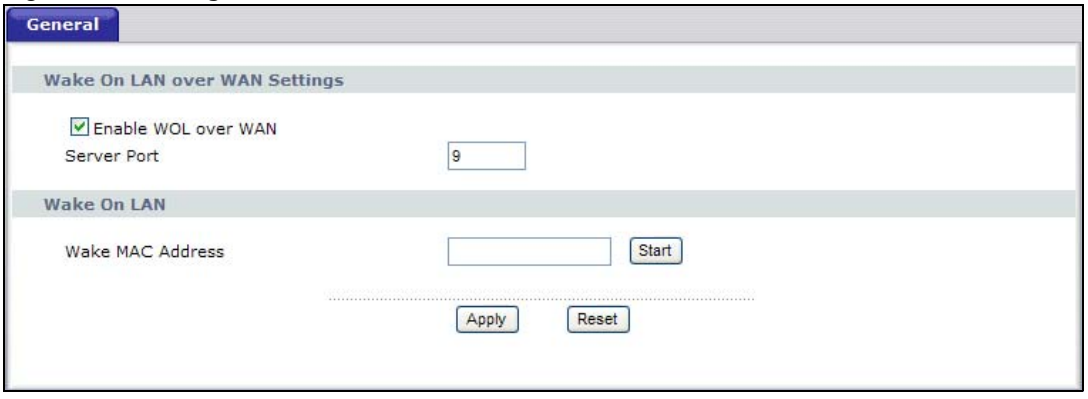
19.1.1 What You Can Do in this Chapter

Use the **WoL** screen (Section 19.2 on page 164) to enable Wake on LAN and remotely turn on a device on the local network.

19.2 The WoL General Screen

Use this screen to remotely turn on a device on the network.Click the **Management > WoL** to open the following screen.

Figure 105 Management > WoL



The following table describes the labels in this screen.

Table 68 Management > WoL

LABEL	DESCRIPTION
Wake On LAN over WAN Settings	
Enable WOL over WAN	Select this option to have the NBG4115 forward a WoL "Magic Packet" to all devices on the LAN if the packet comes from the WAN or remote network and uses the port number specified in the **Server Port** field. A LAN device whose hardware supports Wake on LAN then will be powered on if it is turned off previously.
Server Port	Type a port number from which a WoL packet is forwarded to the LAN.
Wake On LAN	
Wake MAC Address	Enter the MAC Address of the device on the network that will be turned on. A MAC address consists of six hexadecimal character pairs.
Start	Click this to have the NBG4115 generate a WoL packet and forward it to turn the specified device on. A screen pops up displaying MAC address error if you input the MAC address incorrectly.
Apply	Click **Apply** to save the setting to the NBG4115.
Reset	Click **Reset** to begin configuring this screen afresh.

20

NetUSB

20.1 Overview

NetUSB allows you to connect a USB device or USB to the NBG4115 and then share it across your network. You can also connect a wireless 3G USB dongle to the NBG4115 and share high speed 3G access to the Internet across both your LAN or WLAN.

For information on configuring the USB network sharing feature using the ZyXLEL Share Center Utility, see Chapter 2 on page 19.

20.1.1 What You Can Do in this Chapter

Use the **NetUSB** screen (Section 19.2 on page 164) to configure the NetUSB port on the NBG4115.

20.1.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

NetUSB

This is the name of the feature on the NBG4115 that allows you to share USB devices that are connected to the NBG4115 with the rest of the network. NetUSB supports both standard USB devices and 3G USB devices.

USB

This NBG4115 supports both USB v1.0 and v2.0.

Mobile 3G

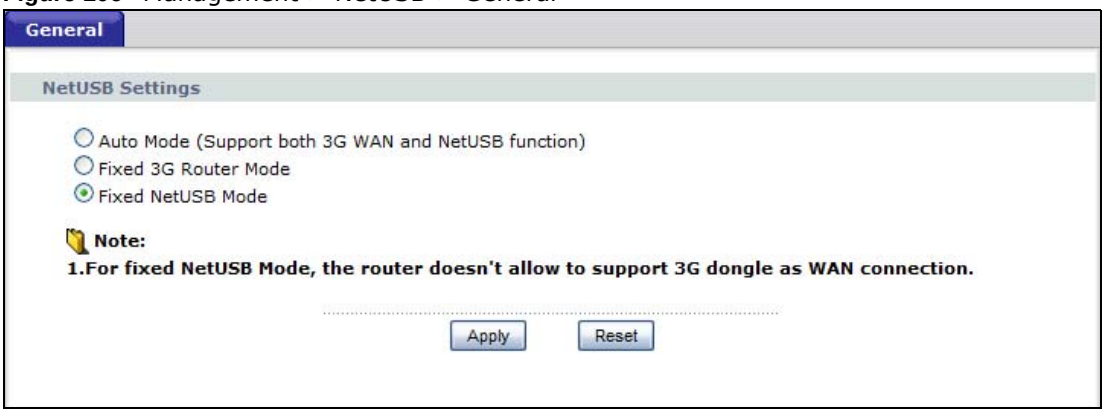
3G is an International Telecommunication Union (ITU) mobile networking standard that provides high-speed connectivity, greater network capacity, and a significantly improved broadcast range to compatible devices.

For more information on configuring 3G, see Chapter 8 on page 97.

20.2 The NetUSB General Screen

Use this screen to configure your NetUSB settings.Click the **Management > NetUSB** to open the following screen.

Figure 106 Management > NetUSB > General


General
NetUSB Settings
Auto Mode (Support both 3G WAN and NetUSB function)
Fixed 3G Router Mode
Fixed NetUSB Mode
Note:
1.For fixed NetUSB Mode, the router doesn't allow to support 3G dongle as WAN connection.
Apply
Reset

The following table describes the labels in this screen.

Table 69 Management > NetUSB > General

LABEL	DESCRIPTION
Auto Mode	Select this to allow the NBG4115 to support both 3G wireless and NetUSB functionality through its USB port. If you connect a USB hub and then a 3G USB dongle, the NBG4115 can support both concurrently.
Fixed 3G Router Mode	Select this to allow the NBG4115 to only support 3G wireless through its USB port.
Fixed NetUSB Mode	Select this to allow the NBG4115 to support only non-3G USB connections through its USB port.
Apply	Click **Apply** to save the setting to the NBG4115.
Reset	Click **Reset** to begin configuring this screen afresh.

21 System

21.1 Overview

This chapter provides information on the **System** screens.

See the chapter about wizard setup for more information on the next few screens.

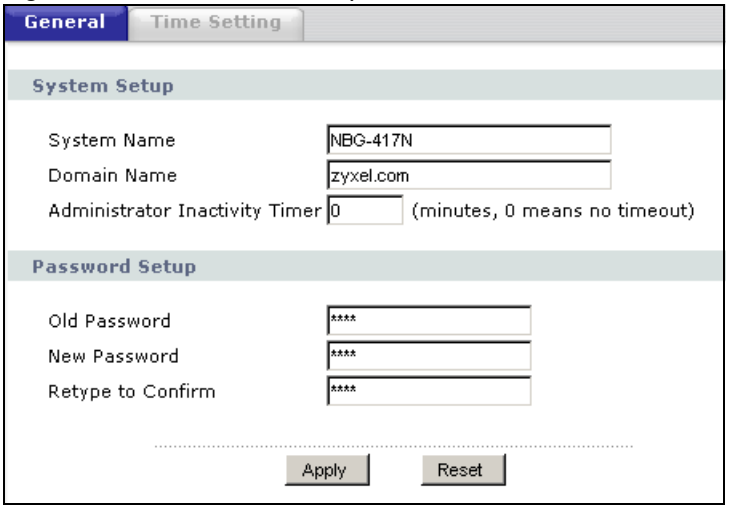
21.1.1 What You Can Do in this Chapter

- Use the **General** screen (Section 21.2 on page 169) to enter a name to identify the NBG4115 in the network and set the password.
- Use the **Time Setting** screen (Section 21.3 on page 171) to change your NBG4115's time and date.

21.2 General

Use this screen to enter a name to identify the NBG4115 in the network and set the password. Click **Maintenance** > **System**. The following screen displays.

Figure 107 Maintenance > System > General



The following table describes the labels in this screen.

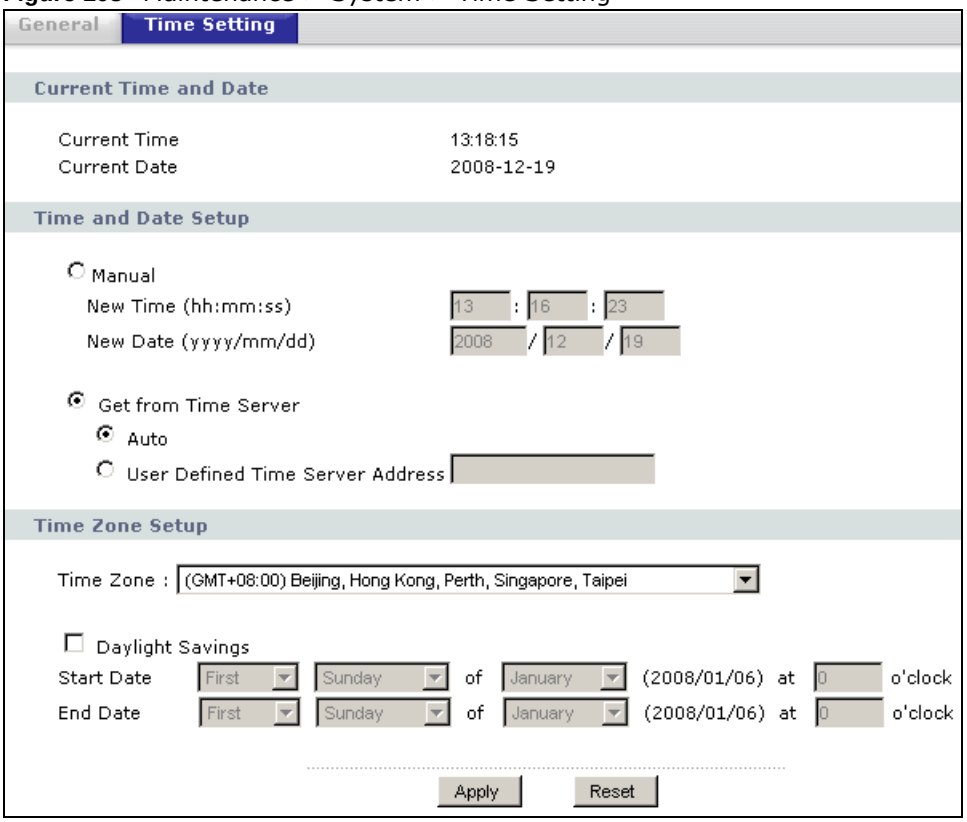
Table 70 Maintenance > System > General

LABEL	DESCRIPTION
System Setup	
System Name	System Name is a unique name to identify the NBG4115 in an Ethernet network. It is recommended you enter your computer's "Computer name" in this field (see the chapter about wizard setup for how to find your computer's name). This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. The domain name entered by you is given priority over the ISP assigned domain name.
Administrator Inactivity Timer	Type how many minutes a management session can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Password Setup	Change your NBG4115's password (recommended) using the fields as shown.
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays an asterisk (*) for each character you type.
Retype to Confirm	Type the new password again in this field.
Apply	Click **Apply** to save your changes back to the NBG4115.
Reset	Click **Reset** to begin configuring this screen afresh.

21.3 Time Setting

To change your NBG4115's time and date, click **Maintenance** > **System** > **Time Setting**. The screen appears as shown. Use this screen to configure the NBG4115's time based on your local time zone.

Figure 108 Maintenance > System > Time Setting



he following table describes the labels in this screen.

Table 71 Maintenance > System > Time Setting

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the time of your NBG4115. Each time you reload this page, the NBG4115 synchronizes the time with the time server.
Current Date	This field displays the date of your NBG4115. Each time you reload this page, the NBG4115 synchronizes the date with the time server.
Time and Date Setup	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, Time Zone and Daylight Saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it.

Table 71 Maintenance > System > Time Setting

LABEL	DESCRIPTION
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you set **Time and Date Setup** to **Manual**, enter the new time in this field and then click **Apply**.
New Date (yyyy/mm/dd)	This field displays the last updated date from the time server or the last date configured manually. When you set **Time and Date Setup** to **Manual**, enter the new date in this field and then click **Apply**.
Get from Time Server	Select this radio button to have the NBG4115 get the time and date from the time server you specified below.
Auto	Select **Auto** to have the NBG4115 automatically search for an available time server and synchronize the date and time with the time server after you click **Apply**.
User Defined Time Server Address	Select **User Defined Time Server Address** and enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Daylight Savings**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the first Sunday of April. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **April** and type 2 in the **o'clock** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Daylight Savings**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the last Sunday of October. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Last**, **Sunday**, **October** and type 2 in the **o'clock** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).

Table 71 Maintenance > System > Time Setting

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the NBG4115.
Reset	Click **Reset** to begin configuring this screen afresh.

22 Logs

22.1 Overview

This chapter contains information about configuring general log settings and viewing the NBG4115's logs. Refer to the appendices for example log message explanations.

The Web Configurator allows you to look at all of the NBG4115's logs in one location.

22.1.1 What You Can Do in this Chapter

Use the **View Log** screen (Section 22.2 on page 174) to see the logs for the activity on your NBG4115.

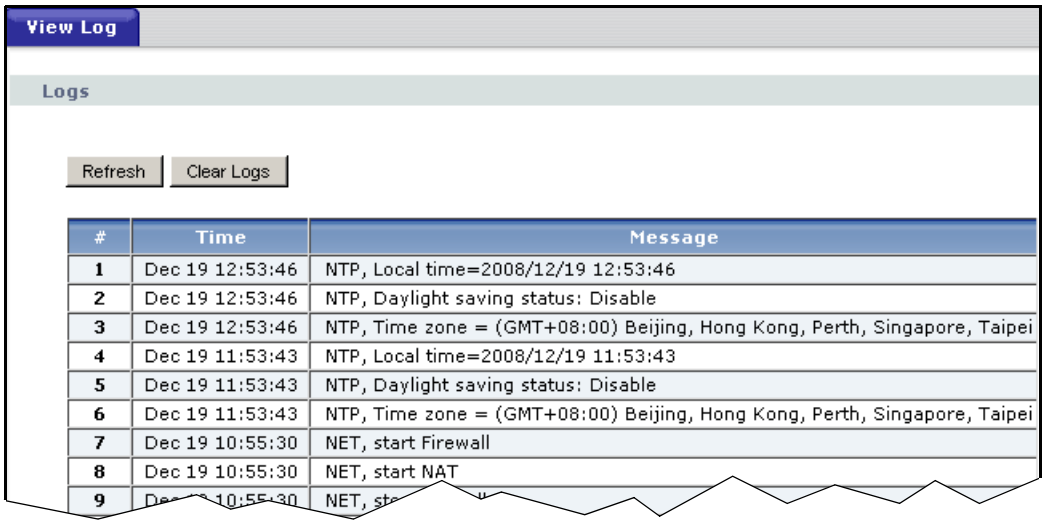
22.2 View Log

Use the **View Log** screen to see the logged messages for the NBG4115.

The log wraps around and deletes the old entries after it fills. Click a column heading to sort it. A triangle indicates ascending or descending sort order.

Click **Maintenance** > **Logs** to open the **View Log** screen.

Figure 109 Maintenance > Logs > View Log


View Log
Logs
Refresh
Clear Logs
Time Message
1 Dec 19 12:53:46 NTP, Local time=2008/12/19 12:53:46
2 Dec 19 12:53:46 NTP, Daylight saving status: Disable
3 Dec 19 12:53:46 NTP, Time zone = (GMT+08:00) Beijing, Hong Kong, Perth, Singapore, Taipei
4 Dec 19 11:53:43 NTP, Local time=2008/12/19 11:53:43
5 Dec 19 11:53:43 NTP, Daylight saving status: Disable
6 Dec 19 11:53:43 NTP, Time zone = (GMT+08:00) Beijing, Hong Kong, Perth, Singapore, Taipei
7 Dec 19 10:55:30 NET, start Firewall
8 Dec 19 10:55:30 NET, start NAT

The following table describes the labels in this screen.

Table 72 Maintenance > Logs > View Log

LABEL	DESCRIPTION
Refresh	Click **Refresh** to renew the log screen.
Clear Log	Click **Clear Log** to delete all the logs.
#	This is the index number of the log entry.
Time	This field displays the time the log was recorded. See the chapter on system maintenance and information to configure the NBG4115's time and date.
Message	This field states the reason for the log.

23 Tools

23.1 Overview

This chapter shows you how to upload a new firmware, upload or save backup configuration files and restart the NBG4115.

23.1.1 What You Can Do in this Chapter

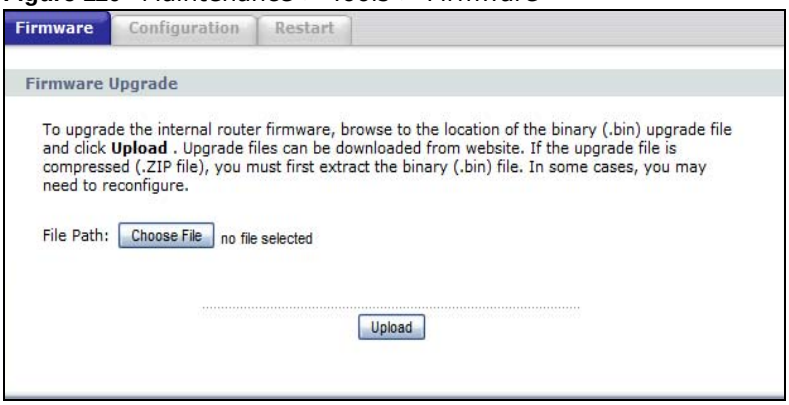
- Use the **Firmware** screen (Section 23.2 on page 176) to upload firmware to your NBG4115.
- Use the **Configuration** screen (Section 23.3 on page 178) to view information related to factory defaults, backup configuration, and restoring configuration.
- Use the **Restart** screen (Section 23.4 on page 180) to have the NBG4115 reboot.

23.2 Firmware

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a "*.bin" extension, e.g., "NBG4115.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Click **Maintenance > Tools**. Follow the instructions in this screen to upload firmware to your NBG4115.

Figure 110 Maintenance > Tools > Firmware


Firmware
Configuration
Restart
Firmware Upgrade
To upgrade the internal router firmware, browse to the location of the binary (.bin) upgrade file and click Upload . Upgrade files can be downloaded from website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.bin) file. In some cases, you may need to reconfigure.
File Path:
Choose File
no file selected
Upload

The following table describes the labels in this screen.

Table 73 Maintenance > Tools > Firmware

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Choose File	Click **Choose File** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.

Note: Do not turn off the NBG4115 while firmware upload is in progress!

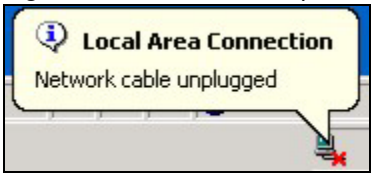
After you see the **Firmware Upload In Process** screen, wait two minutes before logging into the NBG4115 again.

Figure 111 Upload Warning

ZyXEL
Firmware Upload In Process
Please Wait ...
Please wait for the device to finish restarting(PWR LED is on steady). This should take about two minutes. To access the device after a successful firmware upload, you need to log in again. Check your new firmware version in the system status menu.

The NBG4115 automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 112 Network Temporarily Disconnected



After two minutes, log in again and check your new firmware version in the **Status** screen.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Firmware** screen.

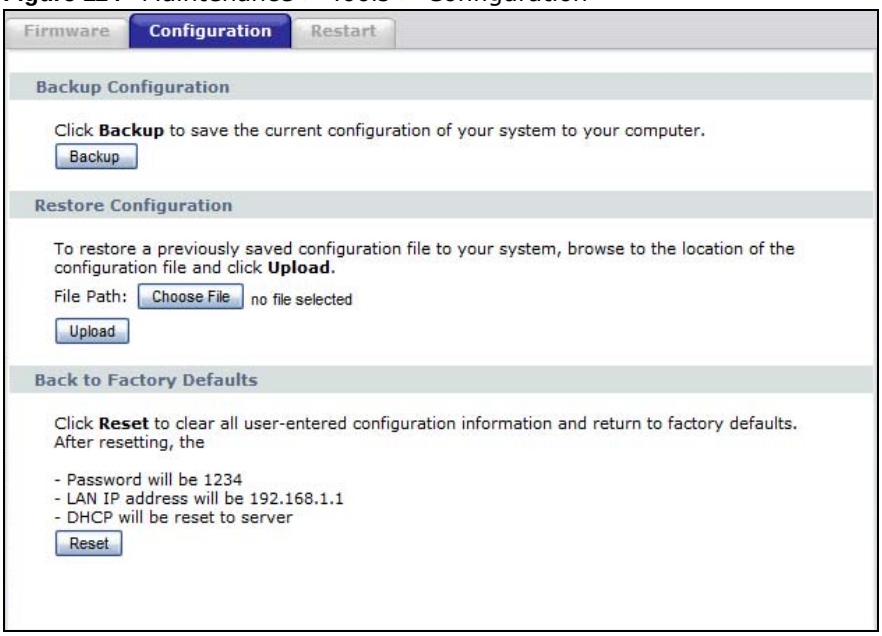
Figure 113 Upload Error Message

system Upload
Firmware upload error!
The uploaded file was not accepted by the device. Please return to the previous page and select a valid upgrade file. Click Help for more information.
Return

23.3 Configuration

Click **Maintenance > Tools** > **Configuration**. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

Figure 114 Maintenance > Tools > Configuration


Firmware
Configuration
Restart
Backup Configuration
Click Backup to save the current configuration of your system to your computer.
Backup
Restore Configuration
To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.
File Path:
Choose File
no file selected
Upload
Back to Factory Defaults
Click Reset to clear all user-entered configuration information and return to factory defaults.
After resetting, the
- Password will be 1234
- LAN IP address will be 192.168.1.1
- DHCP will be reset to server
Reset

23.3.1 Backup Configuration

Backup configuration allows you to back up (save) the NBG4115's current configuration to a file on your computer. Once your NBG4115 is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the NBG4115's current configuration to your computer.

23.3.2 Restore Configuration

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your NBG4115.

Table 74 Maintenance Restore Configuration

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Choose File	Click **Choose File** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process.

Note: Do not turn off the NBG4115 while configuration file upload is in progress

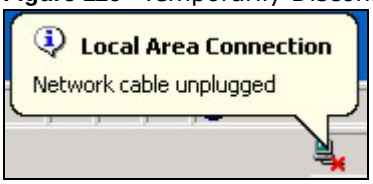
After you see a "configuration upload successful" screen, you must then wait one minute before logging into the NBG4115 again.

Figure 115 Configuration Restore Successful

ZyXEL
Restore Configuration successful
The Device Is Rebooting Now.
After the device finishes rebooting, the login screen displays.

The NBG4115 automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

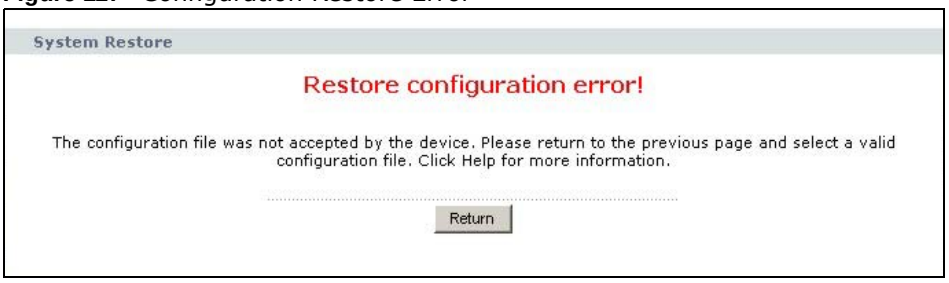
Figure 116 Temporarily Disconnected



If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default NBG4115 IP address (192.168.1.1). See Appendix C on page 215 for details on how to set up your computer's IP address.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Configuration** screen.

Figure 117 Configuration Restore Error


System Restore
Restore configuration error!
The configuration file was not accepted by the device. Please return to the previous page and select a valid configuration file. Click Help for more information.
Return

23.3.3 Back to Factory Defaults

Pressing the **Reset** button in this section clears all user-entered configuration information and returns the NBG4115 to its factory defaults.

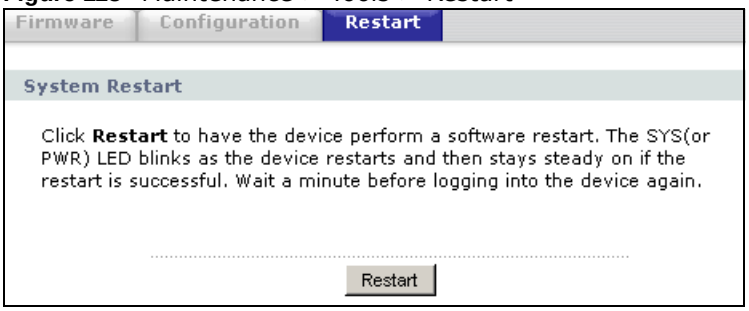
You can also press the **RESET** button on the rear panel to reset the factory defaults of your NBG4115. Refer to the chapter about introducing the Web Configurator for more information on the **RESET** button.

23.4 Restart

System restart allows you to reboot the NBG4115 without turning the power off.

Click **Maintenance > Tools** > **Restart**. Click **Restart** to have the NBG4115 reboot. This does not affect the NBG4115's configuration.

Figure 118 Maintenance > Tools > Restart


Firmware
Configuration
Restart
System Restart
Click Restart to have the device perform a software restart. The SYS(or PWR) LED blinks as the device restarts and then stays steady on if the restart is successful. Wait a minute before logging into the device again.
Restart

24

Sys OP Mode

24.1 Overview

The **Sys OP Mode** (System Operation Mode) function lets you configure whether your NBG4115 is a router or AP. You can choose between **Router Mode** and **AP Mode** depending on your network topology and the features you require from your device. See Section 1.1 on page 15 for more information on which mode to choose.

24.1.1 What You Can Do in this Chapter

Use the General screen (Section 24.2 on page 182) to select how you connect to the Internet.

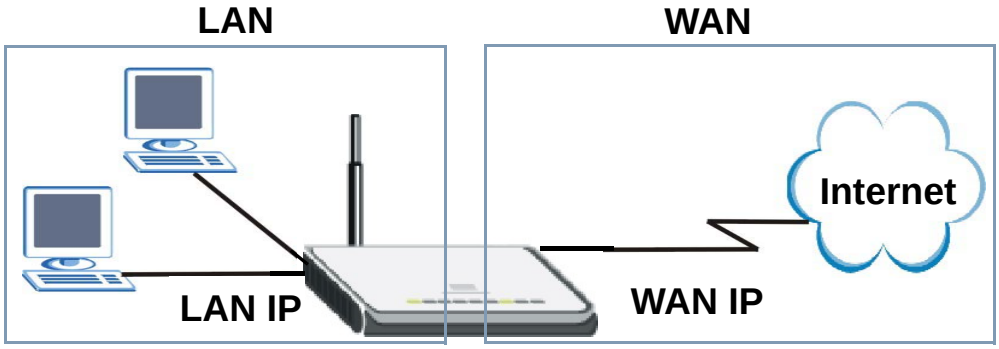
24.1.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

Router

A router connects your local network with another network, such as the Internet. The router has two IP addresses, the LAN IP address and the WAN IP address.

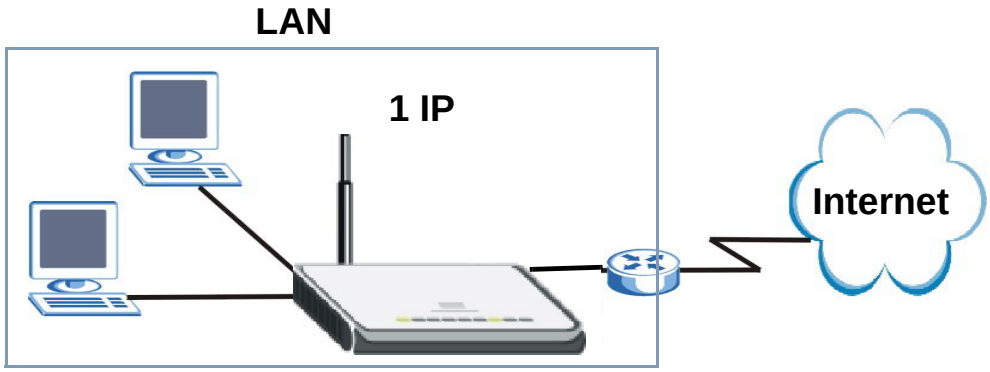
Figure 119 LAN and WAN IP Addresses in Router Mode



AP

An AP extends one network and so has just one IP address. All Ethernet ports on the AP have the same IP address. To connect to the Internet, another device, such as a router, is required.

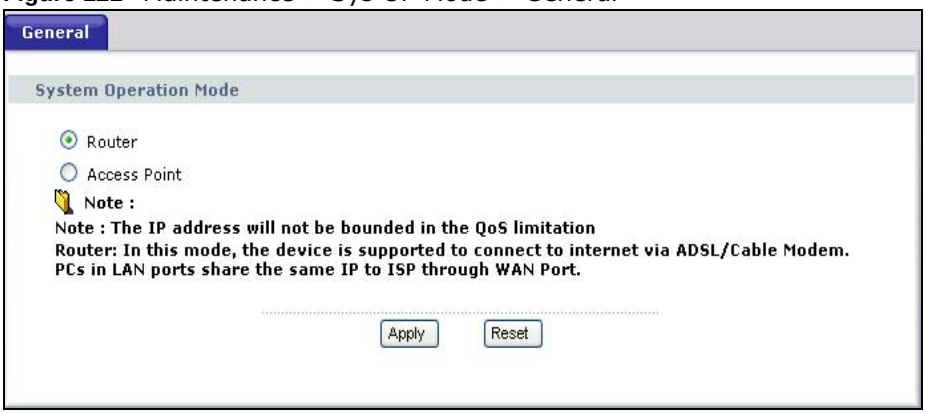
Figure 120 IP Address in AP Mode



24.2 General

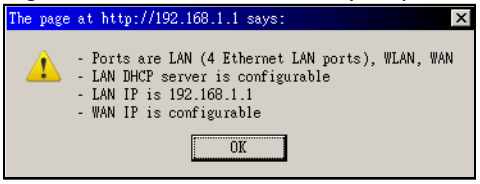
Use this screen to select how you connect to the Internet.

Figure 121 Maintenance > Sys OP Mode > General


General
System Operation Mode
Router
Access Point
Note :
Note : The IP address will not be bounded in the QoS limitation
Router: In this mode, the device is supported to connect to internet via ADSL/Cable Modem.
PCs in LAN ports share the same IP to ISP through WAN Port.
Apply
Reset

If you select Router Mode, the following pop-up message window appears.

Figure 122 Maintenance > Sys Op Mode > General: Router

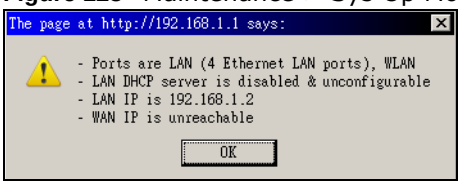

The page at http://192.168.1.1 says:
- Ports are LAN (4 Ethernet LAN ports), WLAN, WAN
- LAN DHCP server is configurable
- LAN IP is 192.168.1.1
- WAN IP is configurable
OK

- In this mode there are both LAN and WAN ports. The LAN Ethernet and WAN Ethernet ports have different IP addresses.
- The DHCP server on your device is enabled and allocates IP addresses to other devices on your local network.

- The LAN IP address of the device on the local network is set to 192.168.1.1.
- You can configure the IP address settings on your WAN port. Contact your ISP or system administrator for more information on appropriate settings.

If you select Access Point the following pop-up message window appears.

Figure 123 Maintenance > Sys Op Mode > General: AP


The page at http://192.168.1.1 says:
- Ports are LAN (4 Ethernet LAN ports), WLAN
- LAN DHCP server is disabled & unconfigurable
- LAN IP is 192.168.1.2
- WAN IP is unreachable
OK

- In **AP Mode** all Ethernet ports have the same IP address.
- All ports on the rear panel of the device are LAN ports, including the port labeled WAN. There is no WAN port.
- The DHCP server on your device is disabled. In AP mode there must be a device with a DHCP server on your network such as a router or gateway which can allocate IP addresses.

The IP address of the device on the local network is set to 192.168.1.2.

The following table describes the labels in the **General** screen.

Table 75 Maintenance > Sys OP Mode > General

LABEL	DESCRIPTION
System Operation Mode	
Router	Select **Router** if your device routes traffic between a local network and another network such as the Internet. This mode offers services such as a firewall or content filter.
Access Point	Select **Access Point** if your device bridges traffic between clients on the same network.
Apply	Click **Apply** to save your settings.
Reset	Click **Reset** to return your settings to the default (**Router**)

Note: If you select the incorrect System Operation Mode you cannot connect to the Internet.

25

Language

25.1 Overview

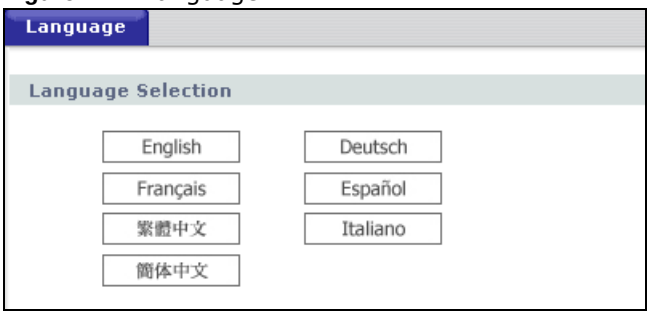
This chapter shows you how to change the Web Configurator’s display language.

25.2 Language

Use this screen to change the language for the Web Configurator display.

Click the language you prefer. The Web Configurator language changes after a while without restarting the NBG4115.

Figure 124 Language



26

Troubleshooting

26.1 Overview

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- NBG4115 Access and Login
- Internet Access
- Resetting the NBG4115 to Its Factory Defaults
- Wireless Router/AP Troubleshooting
- ZyXEL NetUSB Share Center Utility Problems

26.2 Power, Hardware Connections, and LEDs

The NBG4115 does not turn on. None of the LEDs turn on.

1. Make sure you are using the power adaptor or cord included with the NBG4115.
2. Make sure the power adaptor or cord is connected to the NBG4115 and plugged in to an appropriate power source. Make sure the power source is turned on.
3. Disconnect and re-connect the power adaptor or cord to the NBG4115.
4. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.5 on page 16.
2. Check the hardware connections. See the Quick Start Guide.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.
4. Disconnect and re-connect the power adaptor to the NBG4115.

5 If the problem continues, contact the vendor.

26.3 NBG4115 Access and Login

I don't know the IP address of my NBG4115.

1 The default IP address is **192.168.1.1**.

2 If you changed the IP address and have forgotten it, you might get the IP address of the NBG4115 by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the NBG4115 (it depends on the network), so enter this IP address in your Internet browser.Set your device to **Router Mode**, login (see the Quick Start Guide for instructions) and go to the **Device Information** table in the **Status** screen. Your NBG4115's IP address is available in the **Device Information** table.

- If the **DHCP** setting under **LAN information** is **None**, your device has a fixed IP address.
- If the **DHCP** setting under **LAN information** is **Client**, then your device receives an IP address from a DHCP server on the network.

3 If your NBG4115 is a DHCP client, you can find your IP address from the DHCP server. This information is only available from the DHCP server which allocates IP addresses on your network. Find this information directly from the DHCP server or contact your system administrator for more information.

4 Reset your NBG4115 to change all settings back to their default. This means your current settings are lost. See Section 26.5 on page 189 in the **Troubleshooting** for information on resetting your NBG4115.

I forgot the password.

1 The default password is **1234**.

2 If this does not work, you have to reset the device to its factory defaults. See Section 26.5 on page 189.

I cannot see or access the **Login** screen in the Web Configurator.

1 Make sure you are using the correct IP address.

- The default IP address is 192.168.1.1.
- If you changed the IP address (Section 9.3 on page 114), use the new IP address.

- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I don't know the IP address of my NBG4115.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.

3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See Appendix A on page 193.

4 Make sure your computer is in the same subnet as the NBG4115. (If you know that there are routers between your computer and the NBG4115, skip this step.)

- If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See Appendix C on page 215.
- If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the NBG4115. See Appendix C on page 215.

5 Reset the device to its factory defaults, and try to access the NBG4115 with the default IP address. See Section 9.3 on page 114.

6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the NBG4115 using another service, such as Telnet. If you can access the NBG4115, check the remote management settings and firewall rules to find out why the NBG4115 does not respond to HTTP.
- If your computer is connected to the **WAN** port or is connected wirelessly, use a computer that is connected to a **LAN**/**ETHERNET** port.

I can see the **Login** screen, but I cannot log in to the NBG4115.

1 Make sure you have entered the password correctly. The default password is **1234**. This field is case-sensitive, so make sure [Caps Lock] is not on.

2 You cannot log in to the Web Configurator while someone is using Telnet to access the NBG4115. Log out of the NBG4115 in the other session, or ask the person who is logged in to log out.

3 This can happen when you fail to log out properly from your last session. Try logging in again after 5 minutes.

4 Disconnect and re-connect the power adaptor or cord to the NBG4115.

5 If this does not work, you have to reset the device to its factory defaults. See Section 26.5 on page 189.

26.4 Internet Access

I cannot access the Internet.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.
2. Make sure you entered your ISP account information correctly in the wizard. These fields are case-sensitive, so make sure [Caps Lock] is not on.
3. If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.
   - Go to Network > Wireless LAN > General > WDS and check if the NBG4115 is set to bridge mode. Select **Disable** and try to connect to the Internet again.
4. Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
5. Go to Maintenance > Sys OP Mode > General. Check your System Operation Mode setting.
   - Select **Router** if your device routes traffic between a local network and another network such as the Internet.
   - Select **Access Point** if your device bridges traffic between clients on the same network.
6. If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the NBG4115), but my Internet connection is not available anymore.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.5 on page 16.
2. Reboot the NBG4115.
3. If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1. There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.5 on page 16. If the NBG4115 is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
2. Check the signal strength. If the signal strength is low, try moving the NBG4115 closer to the AP if possible, and look around to see if there are any devices that might be interfering with the wireless network (for example, microwaves, other wireless networks, and so on).

3 Reboot the NBG4115.

4 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestion

- Check the settings for QoS. If it is disabled, you might consider activating it.

26.5 Resetting the NBG4115 to Its Factory Defaults

If you reset the NBG4115, you lose all of the changes you have made. The NBG4115 re-loads its default settings, and the password resets to **1234**. You have to make all of your changes again.

You will lose all of your changes when you push the **RESET** button.

To reset the NBG4115:

1 Make sure the power LED is on.

2 Press the **RESET** button for longer than 1 second to restart/reboot the NBG4115.

3 Press the **RESET** button for longer than five seconds to set the NBG4115 back to its factory-default configurations.

If the NBG4115 restarts automatically, wait for the NBG4115 to finish restarting, and log in to the Web Configurator. The password is "1234".

If the NBG4115 does not restart automatically, disconnect and reconnect the NBG4115's power. Then, follow the directions above again.

26.6 Wireless Router/AP Troubleshooting

I cannot access the NBG4115 or ping any computer from the WLAN (wireless AP or router).

1 Make sure the wireless LAN is enabled on the NBG4115

2 Make sure the wireless adapter on the wireless station is working properly.

3 Make sure the wireless adapter installed on your computer is IEEE 802.11 compatible and supports the same wireless standard as the NBG4115.

4 Make sure your computer (with a wireless adapter installed) is within the transmission range of the NBG4115.

5 Check that both the NBG4115 and your wireless station are using the same wireless and wireless security settings.

6 Make sure traffic between the WLAN and the LAN is not blocked by the firewall on the NBG4115.

7 Make sure you allow the NBG4115 to be remotely accessed through the WLAN interface. Check your remote management settings.

- See the chapter on Wireless LAN in the User's Guide for more information.

I set up URL keyword blocking, but I can still access a website that should be blocked.

Make sure that you select the **Enable URL Keyword Blocking** check box in the Content Filtering screen. Make sure that the keywords that you type are listed in the **Keyword List**.

If a keyword that is listed in the **Keyword List** is not blocked when it is found in a URL, customize the keyword blocking using commands. See the Customizing Keyword Blocking URL Checking section in the Content Filter chapter.

I can access the Internet, but I cannot open my network folders.

In the Network > LAN > Advanced screen, make sure **Allow between LAN and WAN** is checked. This is not checked by default to keep the LAN secure.

If you still cannot access a network folder, make sure your account has access rights to the folder you are trying to open.

I can access the Web Configurator after I switched to AP mode.

When you change from router mode to AP mode, your computer must have an IP address in the range between "192.168.1.3" and "192.168.1.254".

Refer to Appendix C on page 215 for instructions on how to change your computer's IP address.

26.7 ZyXEL NetUSB Share Center Utility Problems

I cannot access or see a USB device that is connected to the NBG4115.

1. Disconnect the problematic USB device, then reconnect it to the NBG4115.
2. Ensure that the USB device in question has power.
3. Check your cable connections.
4. Restart the NBG4115 by disconnecting the power and then reconnecting it.
5. If the USB device requires a special driver, install the driver from the installation disc that came with the device. After driver installation, reconnect the USB device to the NBG4115 and try to connect to it again with your computer.
6. If the problem persists, contact your vendor.

I cannot install the ZyXEL NetUSB Share Center Utility.

1. Make sure that the set up program is one required for your operating system.
2. Install the latest patches and updates for your operating system.
3. Check the zyxel.com download site for a newer version of the utility.

A

Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Note: The screens used below belong to Internet Explorer version 6, 7 and 8. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

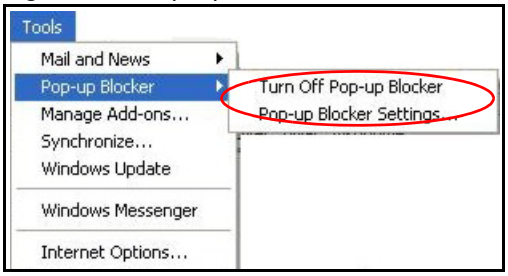
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable Pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 125 Pop-up Blocker



You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 126 Internet Options: Privacy

3 Click **Apply** to save this setting.

Enable Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings...**to open the **Pop-up Blocker Settings** screen.

Figure 127 Internet Options: Privacy

3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.167.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 128 Pop-up Blocker Settings

Pop-up Blocker Settings
Exceptions
Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.
Address of Web site to allow:
http://192.168.1.1
Add
Allowed sites:
Remove
Remove All
Notifications and Filter Level
Play a sound when a pop-up is blocked.
Show Information Bar when a pop-up is blocked.
Filter Level:
Medium: Block most automatic pop-ups
Pop-up Blocker FAQ
Close

5 Click **Close** to return to the **Privacy** screen.

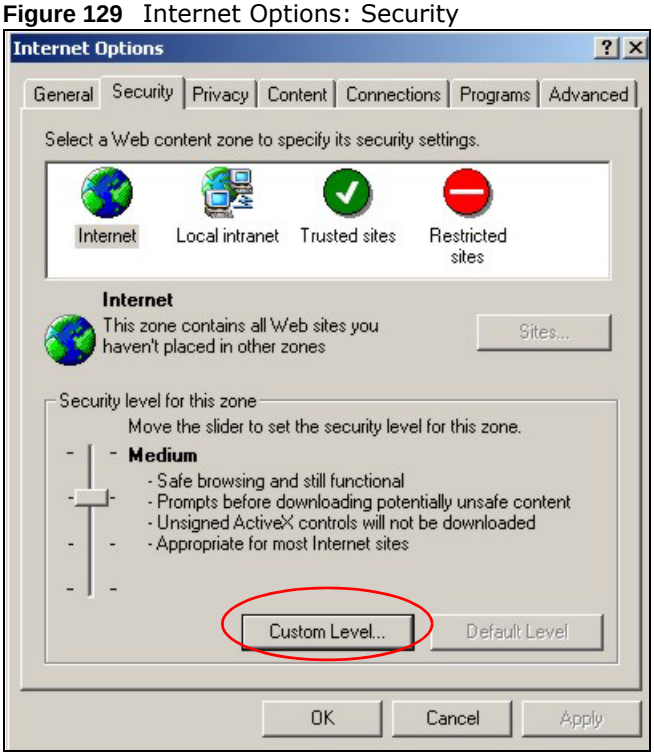
6 Click **Apply** to save this setting.

JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 129 Internet Options: Security



2 Click the **Custom Level...** button.

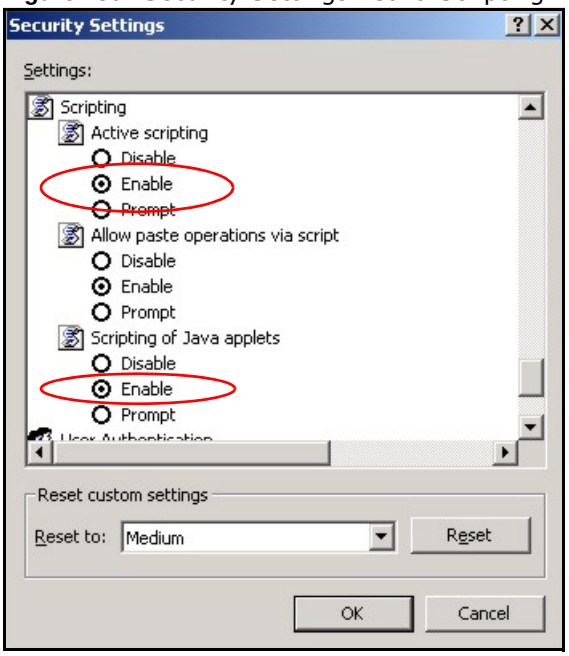
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

Figure 130 Security Settings - Java Scripting



Java Permissions

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

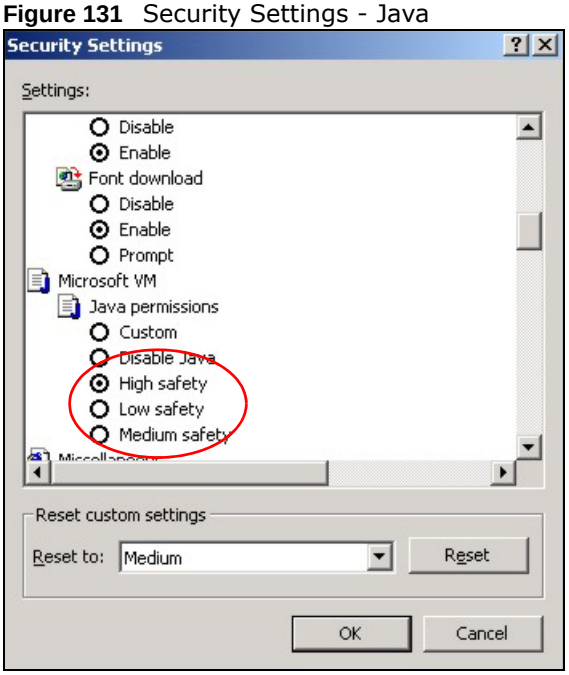
2 Click the **Custom Level...** button.

3 Scroll down to **Microsoft VM**.

4 Under **Java permissions** make sure that a safety level is selected.

5 Click **OK** to close the window.

Figure 131 Security Settings - Java



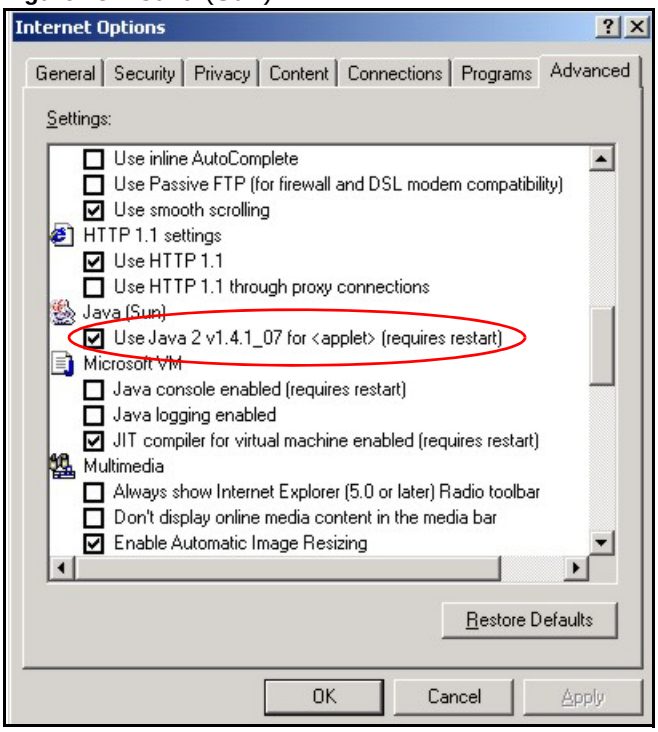
JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.

2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3 Click **OK** to close the window.

Figure 132 Java (Sun)

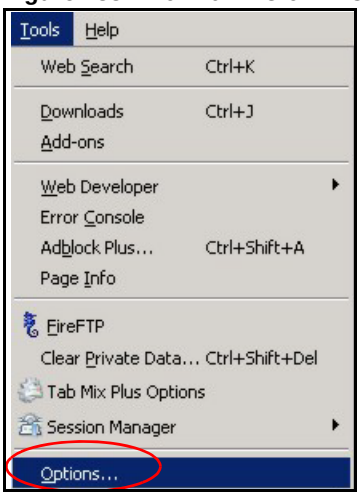


Mozilla Firefox

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary slightly. The steps below apply to Mozilla Firefox 3.0 as well.

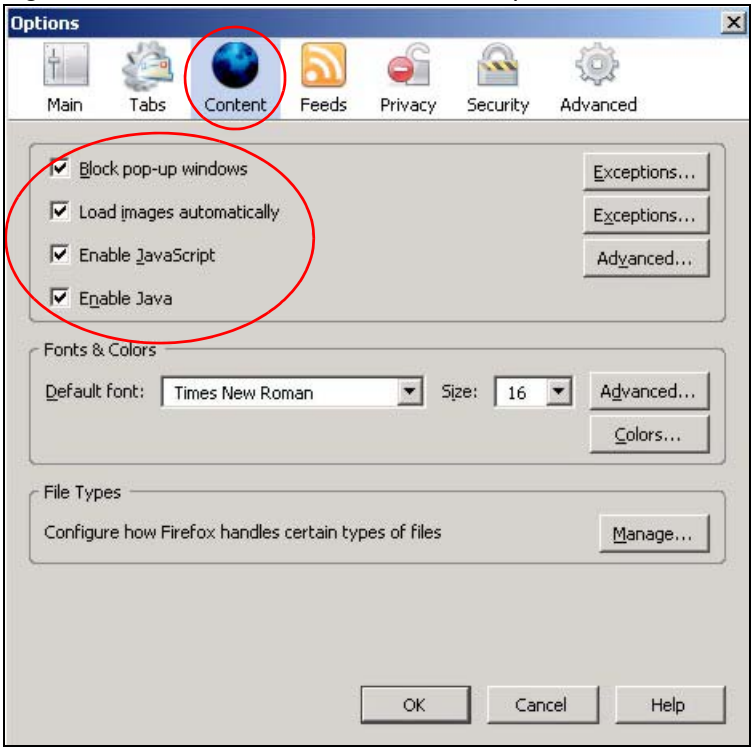
You can enable Java, Javascripts and pop-ups in one screen. Click **Tools,** then click **Options** in the screen that appears.

Figure 133 Mozilla Firefox: TOOLS > Options



Click **Content** to show the screen below. Select the check boxes as shown in the following screen.

Figure 134 Mozilla Firefox Content Security



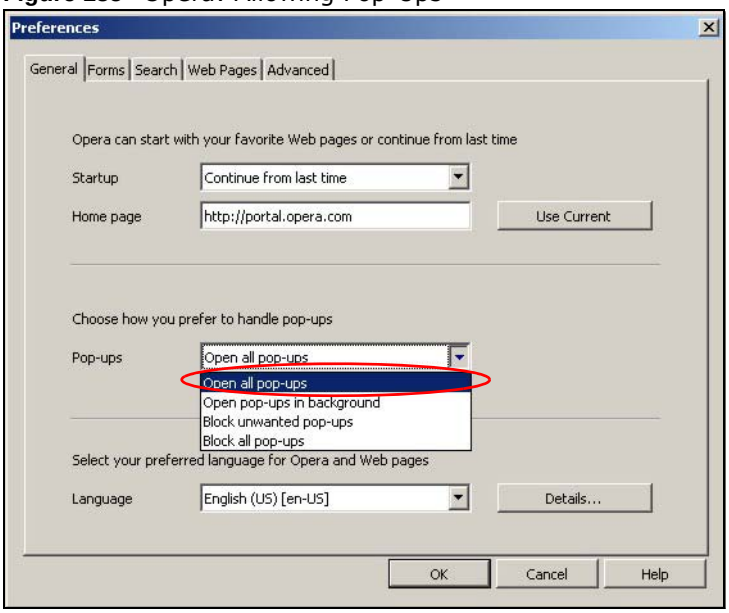
Opera

Opera 10 screens are used here. Screens for other versions may vary slightly.

Allowing Pop-Ups

From Opera, click **Tools**, then **Preferences**. In the **General** tab, go to **Choose how you prefer to handle pop-ups** and select **Open all pop-ups**.

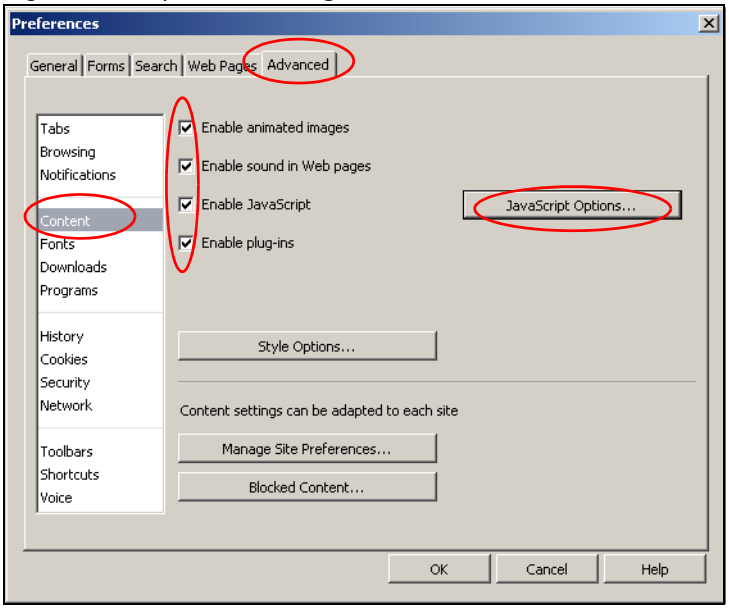
Figure 135 Opera: Allowing Pop-Ups



Enabling Java

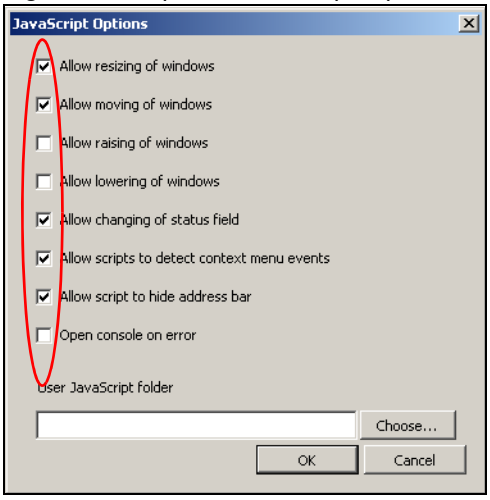
From Opera, click **Tools**, then **Preferences**. In the **Advanced** tab, select **Content** from the left-side menu. Select the check boxes as shown in the following screen.

Figure 136 Opera: Enabling Java



To customize JavaScript behavior in the Opera browser, click **JavaScript Options**.

Figure 137 Opera: JavaScript Options



Select the items you want Opera's JavaScript to apply.

B

IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

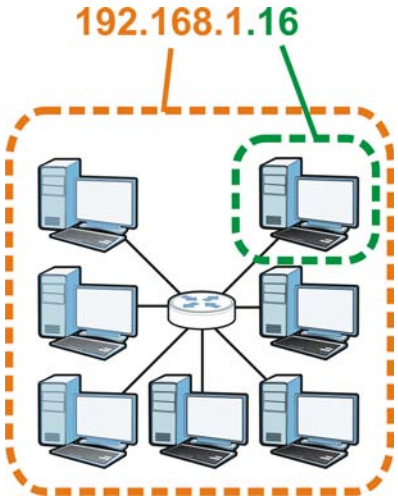
Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 138 Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term "subnet" is short for "sub-network".

A subnet mask has 32 bits. If a bit in the subnet mask is a "1" then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is "0" then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 76 IP Address Network Number and Host ID Example

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	**11111111**	**11111111**	**11111111**	00000000
Network Number	**11000000**	**10101000**	**00000001**	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a "1" value). For example, an "8-bit mask" means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 77 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 78 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} - 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} - 2$	65534
24 bits	255.255.255.0	8 bits	$2^{8} - 2$	254
29 bits	255.255.255.248	3 bits	$2^{3} - 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 79 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192

Table 79 Alternative Subnet Mask Notation (continued)

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

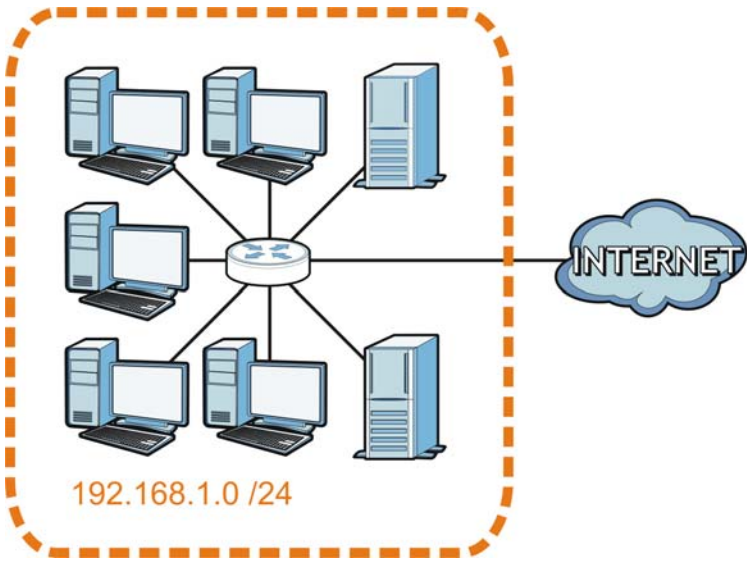
Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of 2^8 – 2 or 254 possible hosts.

The following figure shows the company network before subnetting.

Figure 139 Subnetting Example: Before Subnetting

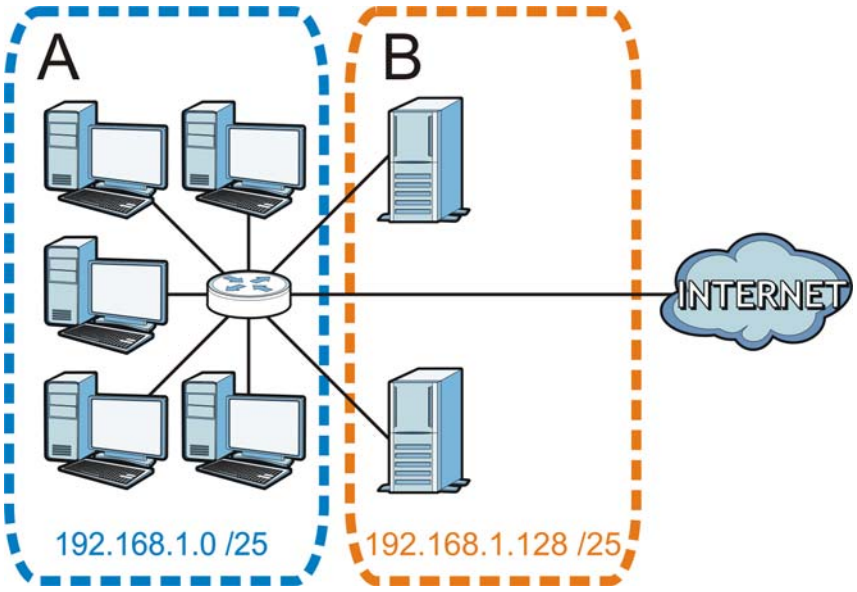


You can "borrow" one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The "borrowed" host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Figure 140 Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of 2^7 – 2 or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving 2^6 - 2 or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 80 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000

Table 80 Subnet 1 (continued)

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 81 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 82 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 83 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

Table 84 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 85 24-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 86 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14

Table 86 16-bit Network Number Subnet Planning (continued)

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the NBG4115.

Once you have decided on the network number, pick an IP address for your NBG4115 that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your NBG4115 will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the NBG4115 unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

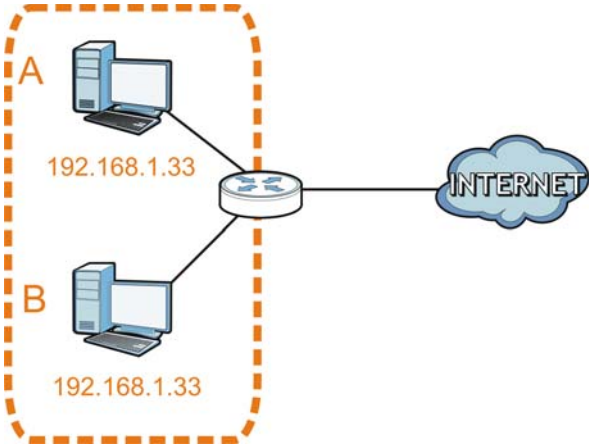
IP Address Conflicts

Each device on a network must have a unique IP address. Devices with duplicate IP addresses on the same network will not be able to access the Internet or other resources. The devices may also be unreachable through the network.

Conflicting Computer IP Addresses Example

More than one device can not use the same IP address. In the following example computer **A** has a static (or fixed) IP address that is the same as the IP address that a DHCP server assigns to computer **B** which is a DHCP client. Neither can access the Internet. This problem can be solved by assigning a different static IP address to computer **A** or setting computer **A** to obtain an IP address automatically.

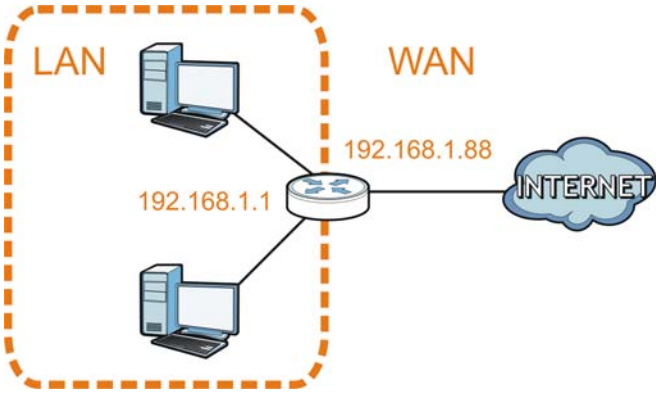
Figure 141 Conflicting Computer IP Addresses Example



Conflicting Router IP Addresses Example

Since a router connects different networks, it must have interfaces using different network numbers. For example, if a router is set between a LAN and the Internet (WAN), the router's LAN and WAN addresses must be on different subnets. In the following example, the LAN and WAN are on the same subnet. The LAN computers cannot access the Internet because the router cannot route between networks.

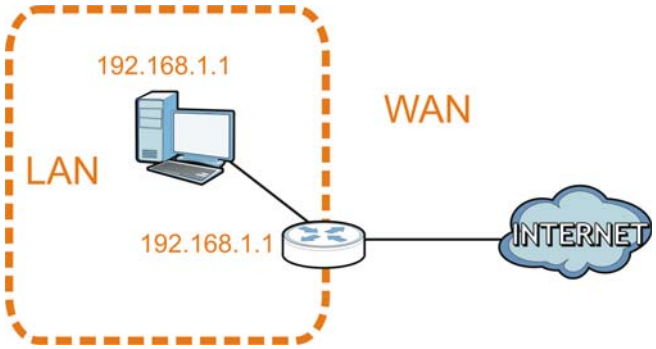
Figure 142 Conflicting Router IP Addresses Example



Conflicting Computer and Router IP Addresses Example

More than one device can not use the same IP address. In the following example, the computer and the router's LAN port both use 192.168.1.1 as the IP address. The computer cannot access the Internet. This problem can be solved by assigning a different IP address to the computer or the router's LAN port.

Figure 143 Conflicting Computer and Router IP Addresses Example



C

Setting Up Your Computer's IP Address

Note: Your specific NBG4115 may not support all of the operating systems described in this appendix. See the product specifications for more information about which operating systems are supported.

This appendix shows you how to configure the IP settings on your computer in order for it to be able to communicate with the other devices on your network. Windows Vista/XP/2000, Mac OS 9/OS X, and all versions of UNIX/LINUX include the software components you need to use TCP/IP on your computer.

If you manually assign IP information instead of using a dynamic IP, make sure that your network's computers have IP addresses that place them in the same subnet.

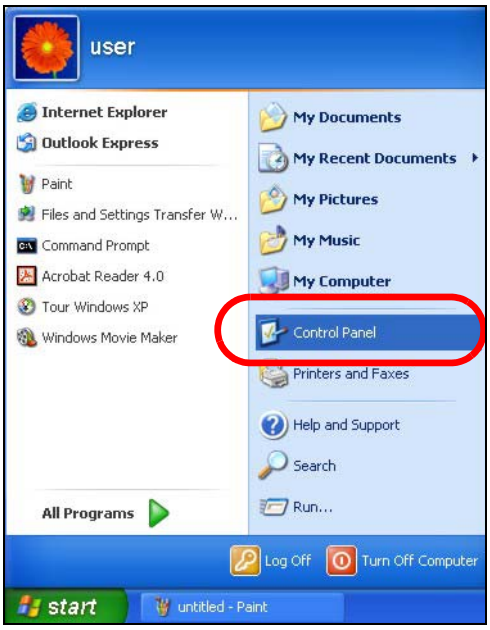
In this appendix, you can set up an IP address for:

- Windows XP/NT/2000 on page 216
- Windows Vista on page 219
- Windows 7 on page 223
- Mac OS X: 10.3 and 10.4 on page 227
- Mac OS X: 10.5 and 10.6 on page 230
- Linux: Ubuntu 8 (GNOME) on page 233
- Linux: openSUSE 10.3 (KDE) on page 237

Windows XP/NT/2000

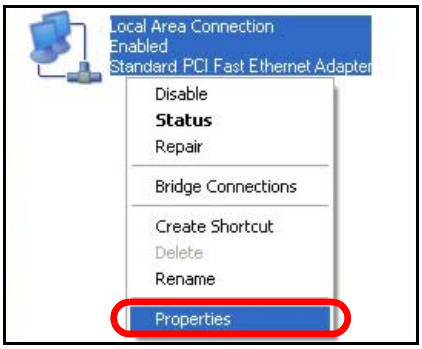
The following example uses the default Windows XP display theme but can also apply to Windows 2000 and Windows NT.

1 Click **Start** > **Control Panel**.

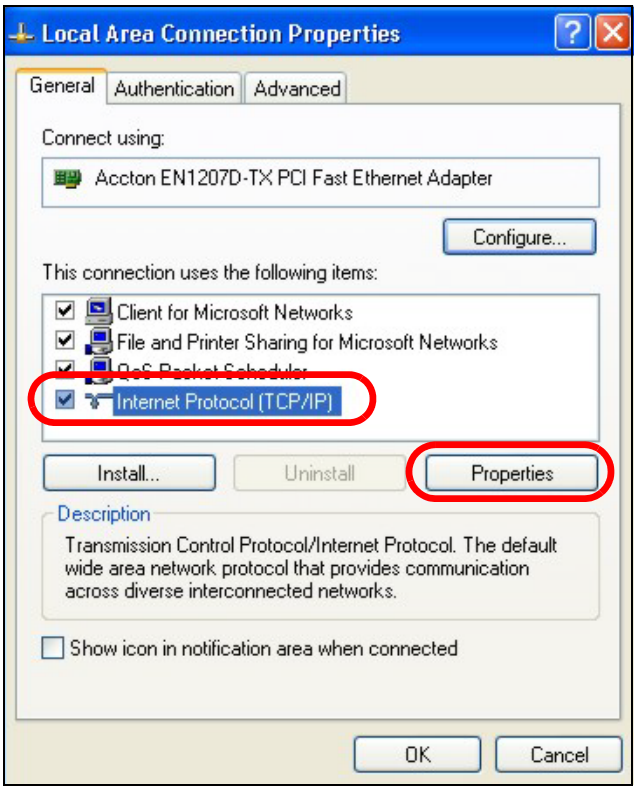


2 In the **Control Panel**, click the **Network Connections** icon.

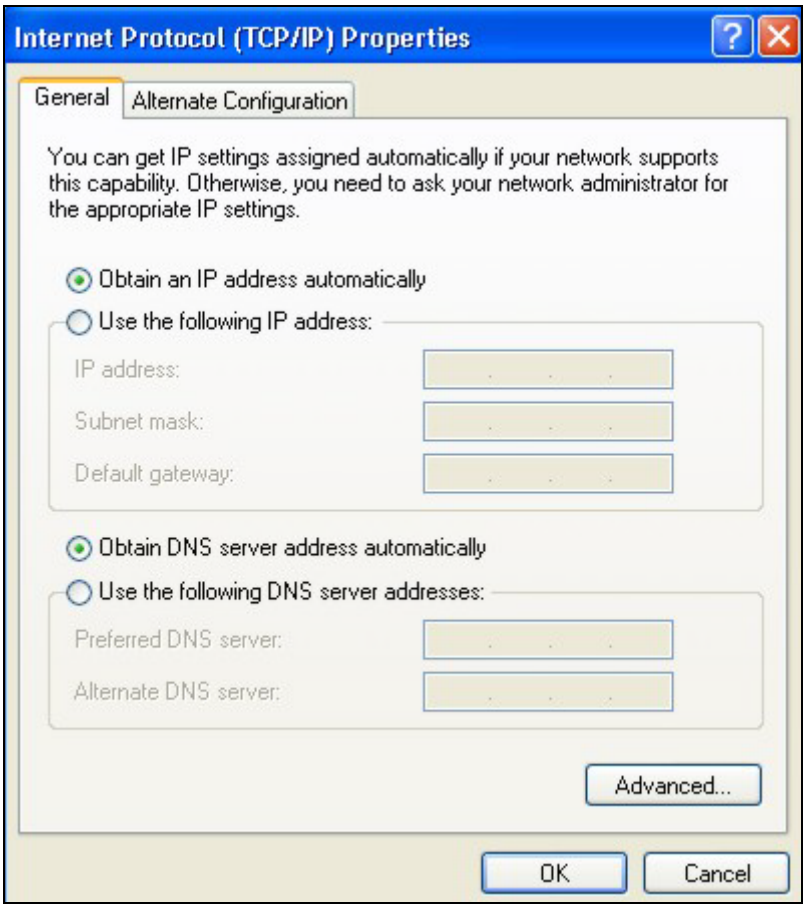
3 Right-click **Local Area Connection** and then select **Properties**.



4 On the **General** tab, select **Internet Protocol (TCP/IP)** and then click **Properties**.



5 The **Internet Protocol TCP/IP Properties** window opens.


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

6 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided.

7 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

8 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

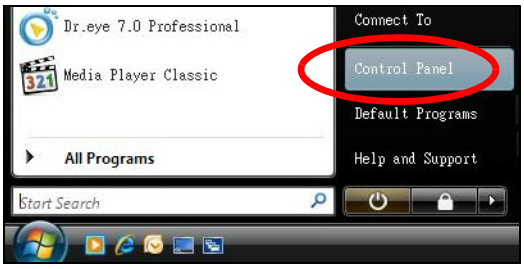
2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

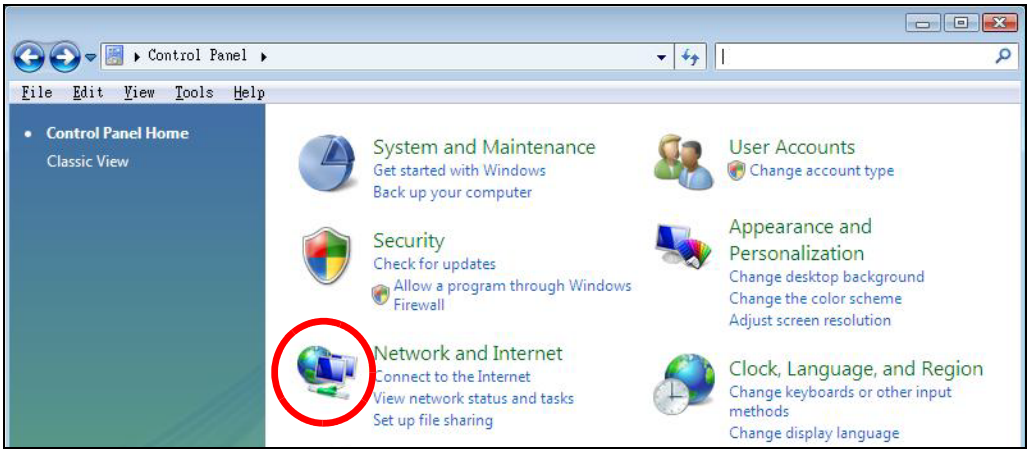
Windows Vista

This section shows screens from Windows Vista Professional.

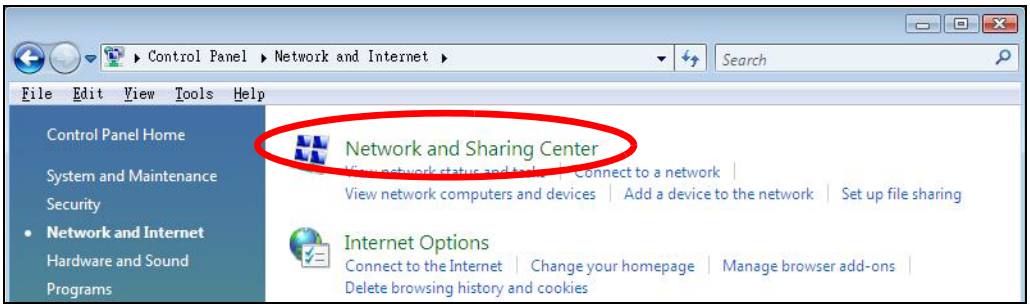
1 Click **Start** > **Control Panel**.



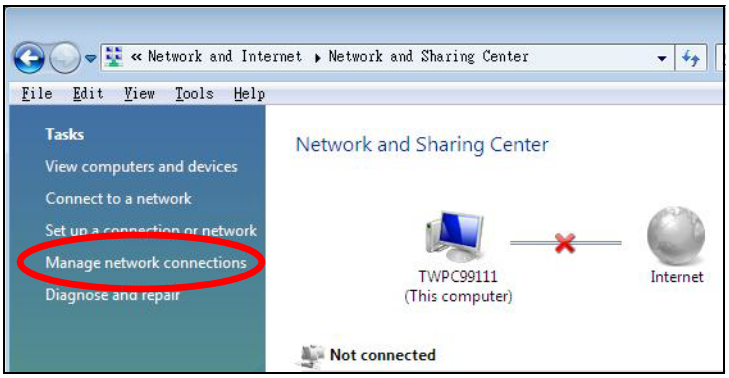
2 In the **Control Panel**, click the **Network and Internet** icon.



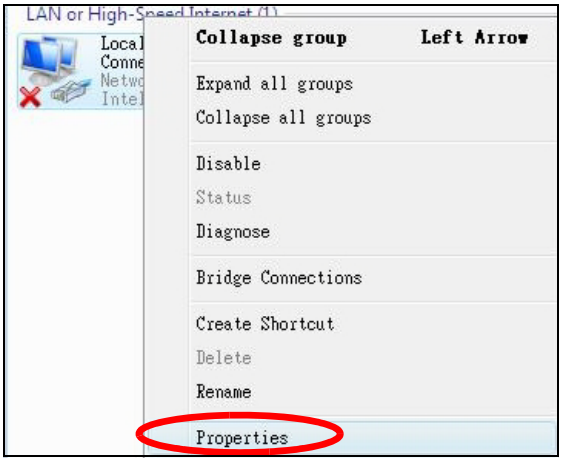
3 Click the **Network and Sharing Center** icon.



4 Click **Manage network connections**.

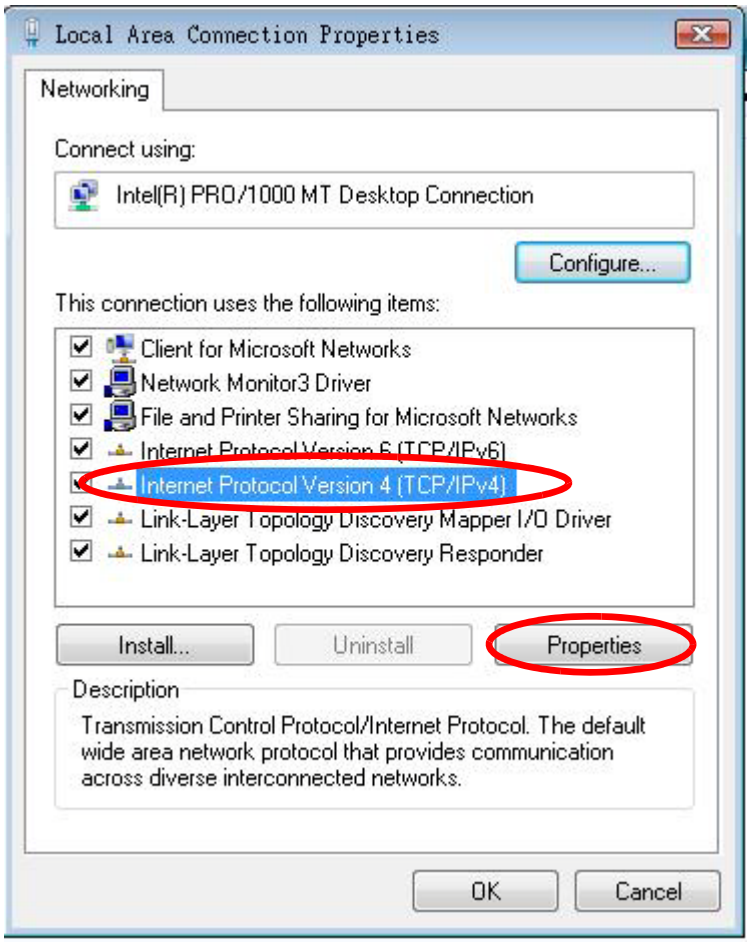


5 Right-click **Local Area Connection** and then select **Properties**.

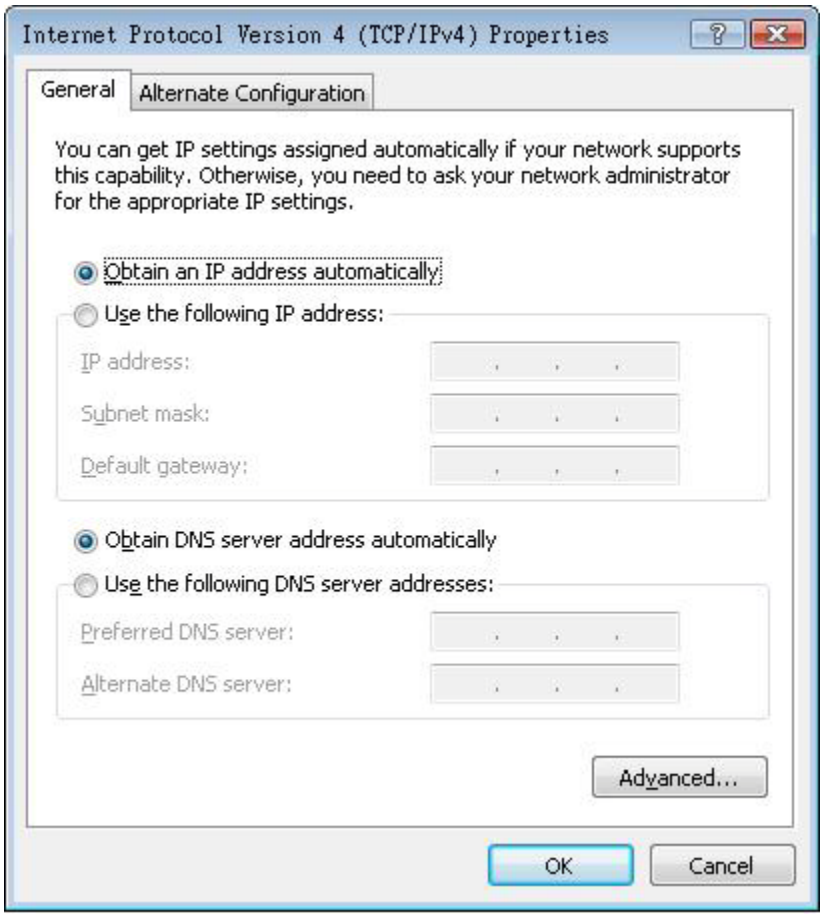


Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

6 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.



7 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.


Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

8 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided.Click **Advanced**.

9 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

10 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

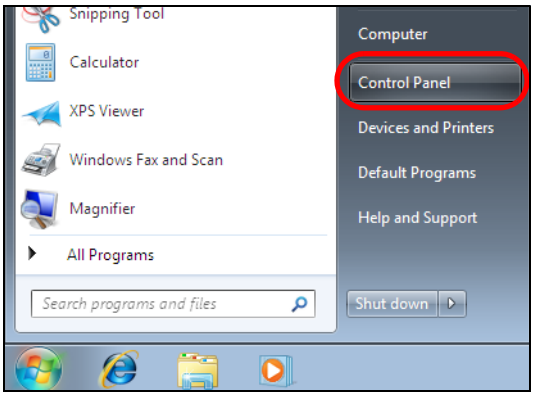
2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

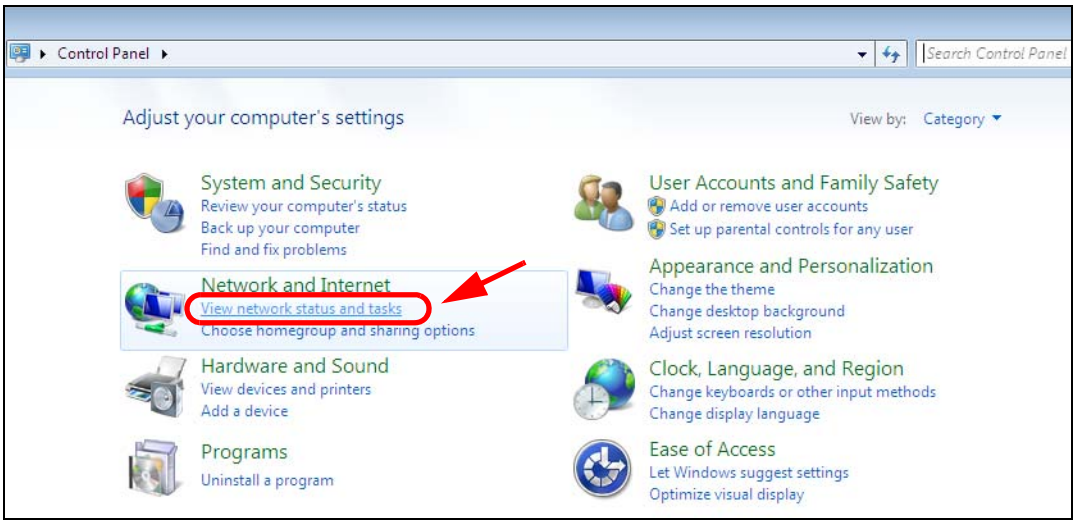
Windows 7

This section shows screens from Windows 7 Enterprise.

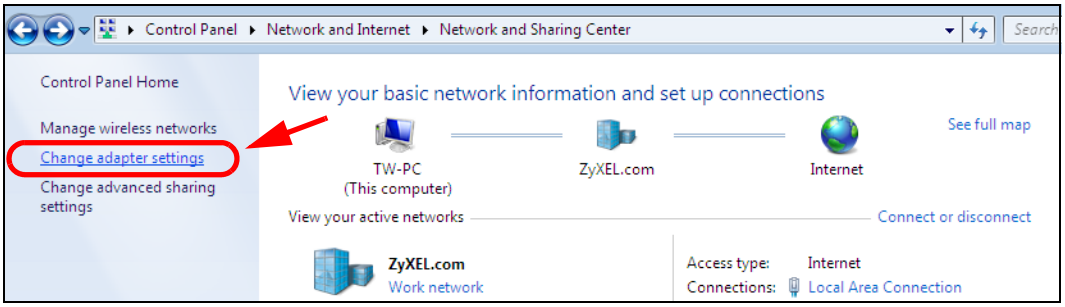
1 Click **Start** > **Control Panel**.



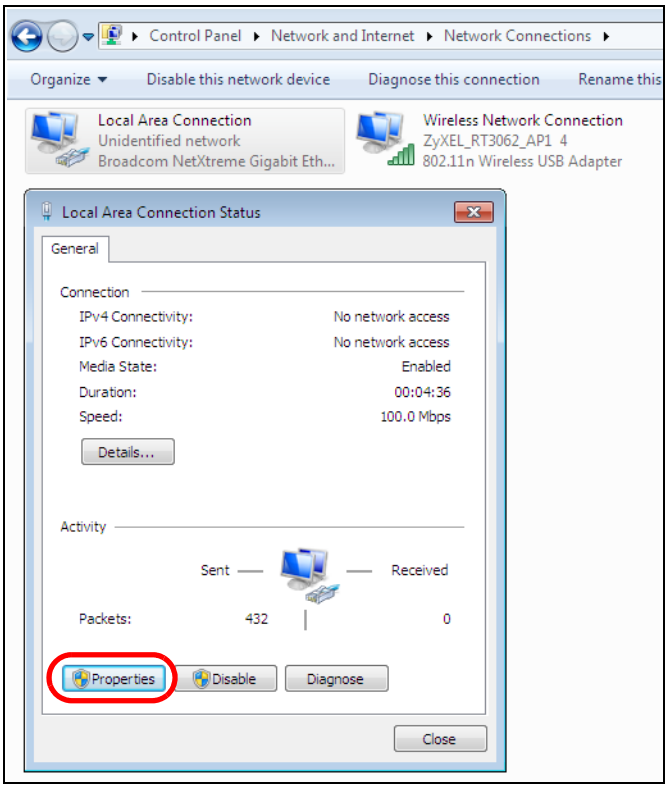
2 In the **Control Panel**, click **View network status and tasks** under the **Network and Internet** category.



3 Click **Change adapter settings**.

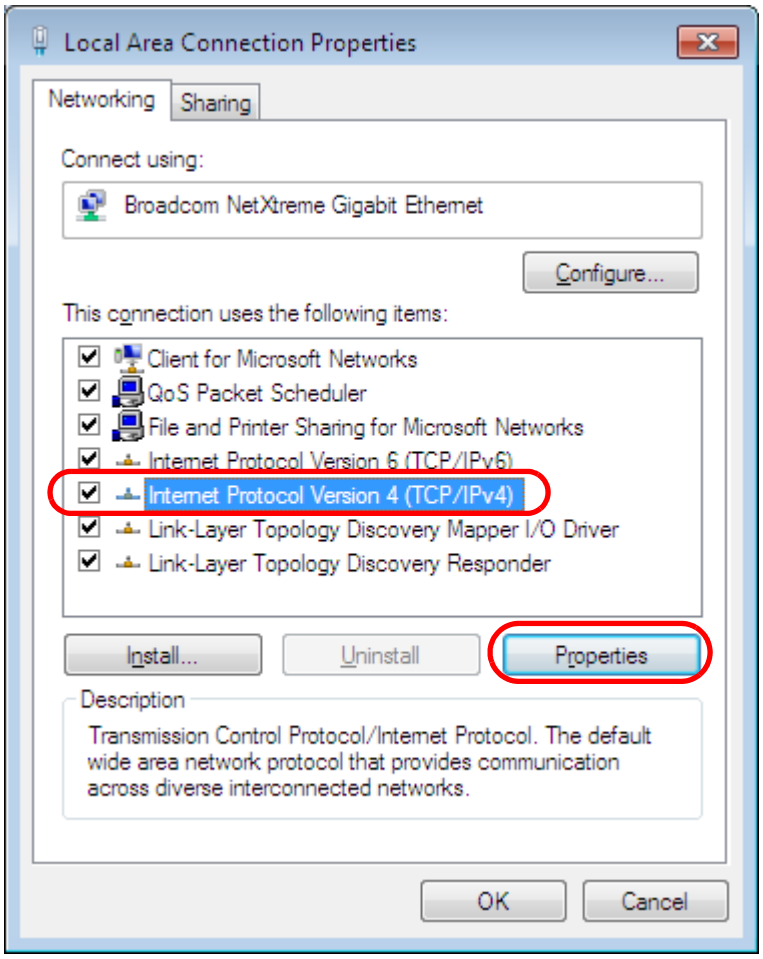


4 Double click **Local Area Connection** and then select **Properties**.

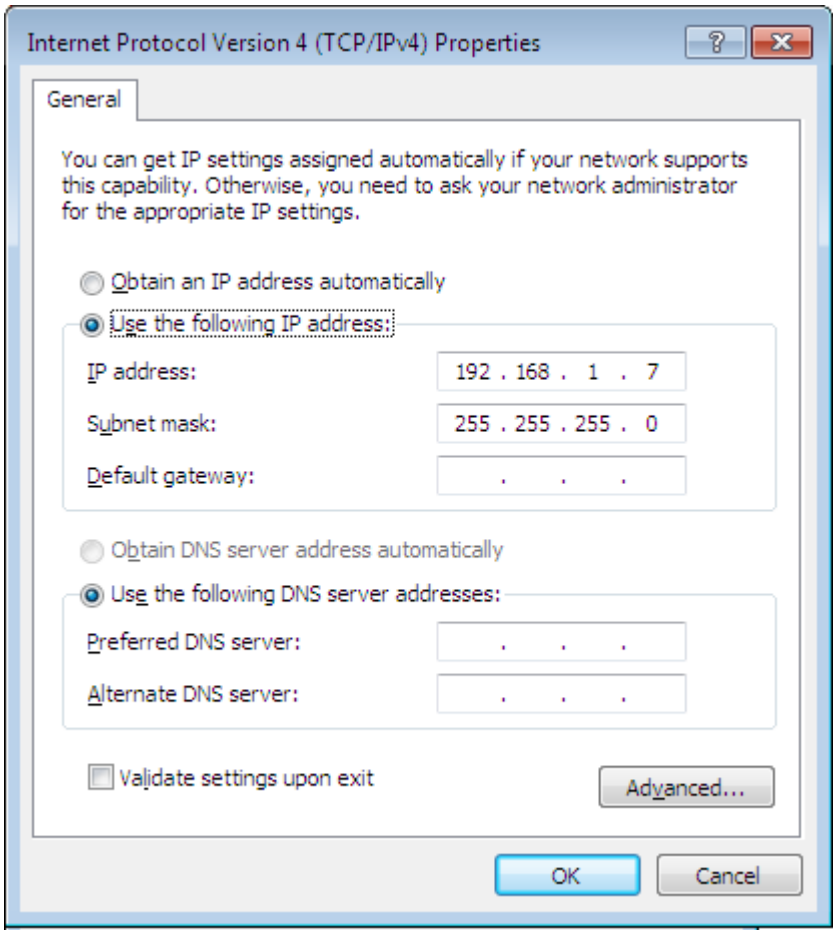


Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

5 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.



6 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.


Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 1 . 7
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

7 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided. Click **Advanced** if you want to configure advanced settings for IP, DNS and WINS.

8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

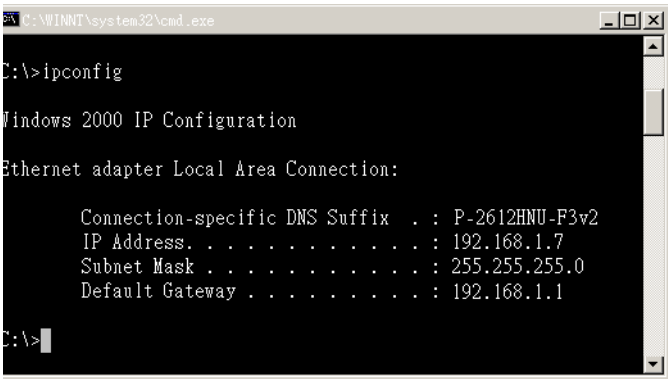
9 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

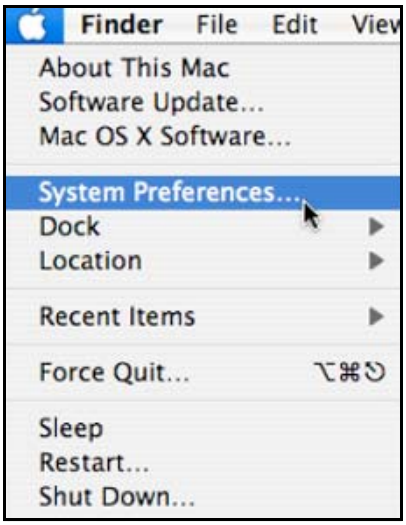
3 The IP settings are displayed as follows.


C:\WINNT\system32\cmd.exe
C:\>ipconfig
Windows 2000 IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . : P-2612HNU-F3v2
IP Address. . . . . : 192.168.1.7
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
C:\>

Mac OS X: 10.3 and 10.4

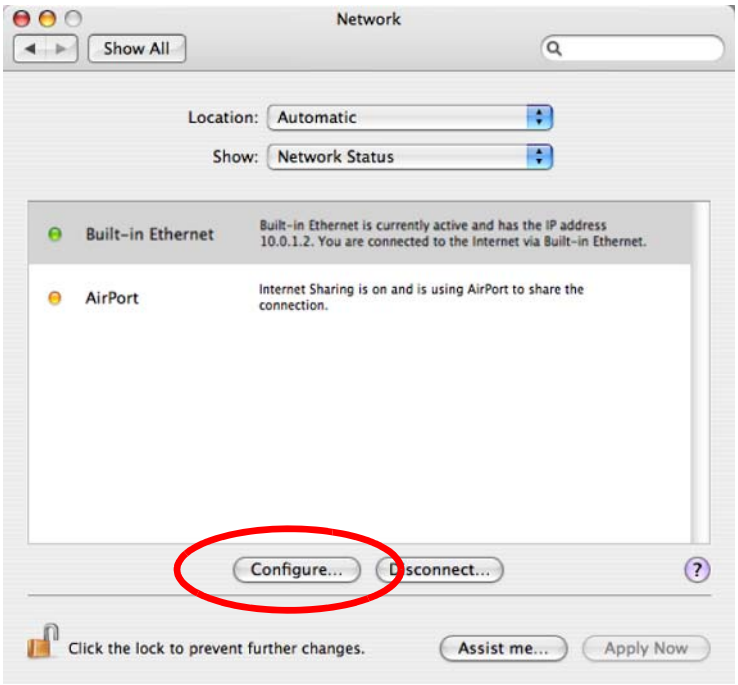
The screens in this section are from Mac OS X 10.4 but can also apply to 10.3.

1 Click **Apple** > **System Preferences**.

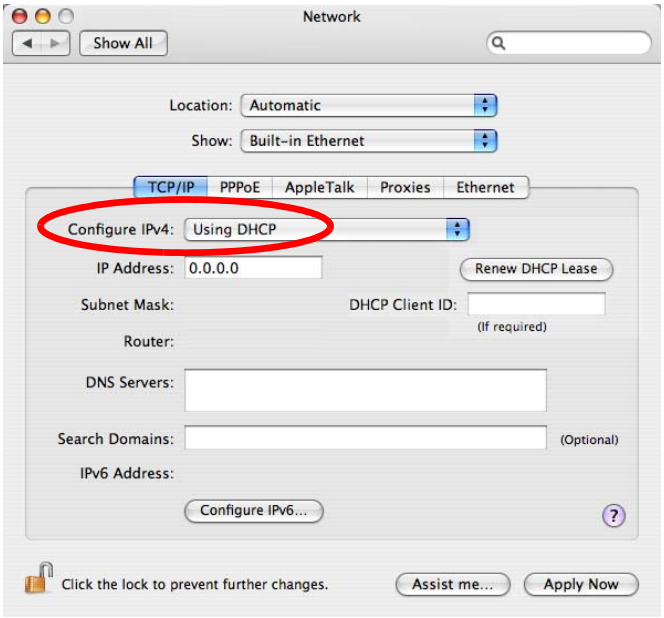


2 In the **System Preferences** window, click the **Network** icon.

3 When the **Network** preferences pane opens, select **Built-in Ethernet** from the network connection type list, and then click **Configure.**

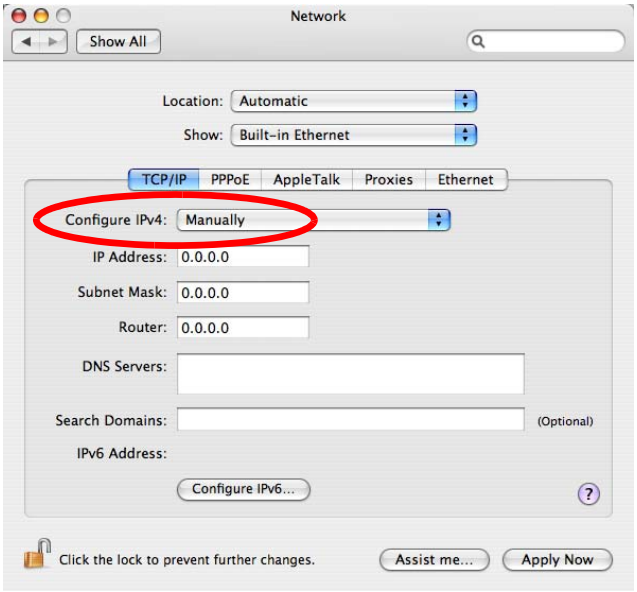

Network
Show All
Location: Automatic
Show: Network Status
Built-in Ethernet
Built-in Ethernet is currently active and has the IP address 10.0.1.2. You are connected to the Internet via Built-in Ethernet.
AirPort
Internet Sharing is on and is using AirPort to share the connection.
Configure...
Disconnect...
Click the lock to prevent further changes.
Assist me...
Apply Now

4 For dynamically assigned settings, select **Using DHCP** from the **Configure IPv4** list in the **TCP/IP** tab.



5 For statically assigned settings, do the following:

- From the **Configure IPv4** list, select **Manually**.
- In the **IP Address** field, type your IP address.
- In the **Subnet Mask** field, type your subnet mask.
- In the **Router** field, type the IP address of your device.

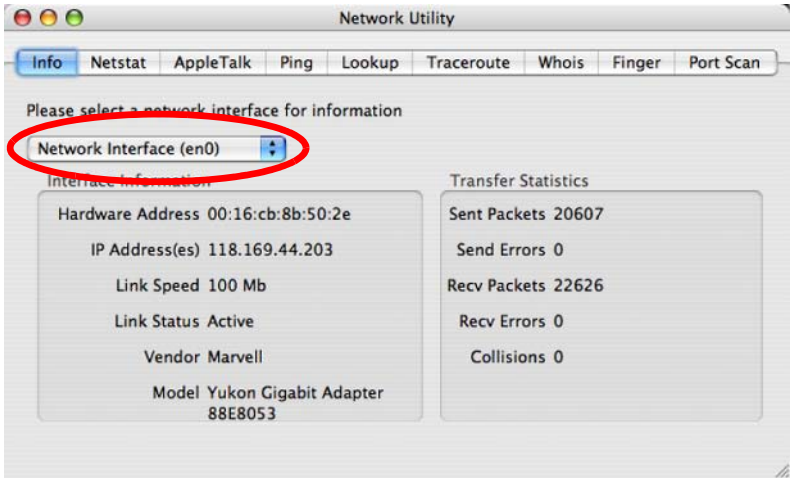


6 Click **Apply Now** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network Interface** from the **Info** tab.

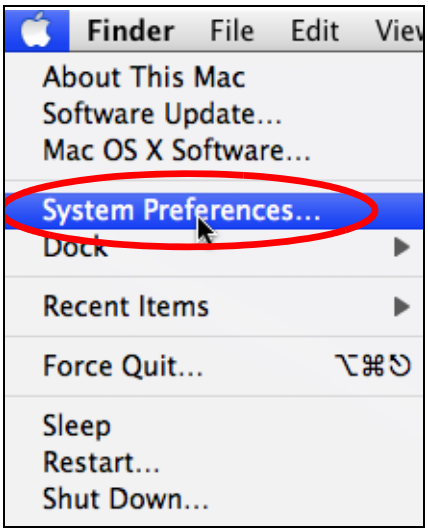
Figure 144 Mac OS X 10.4: Network Utility



Mac OS X: 10.5 and 10.6

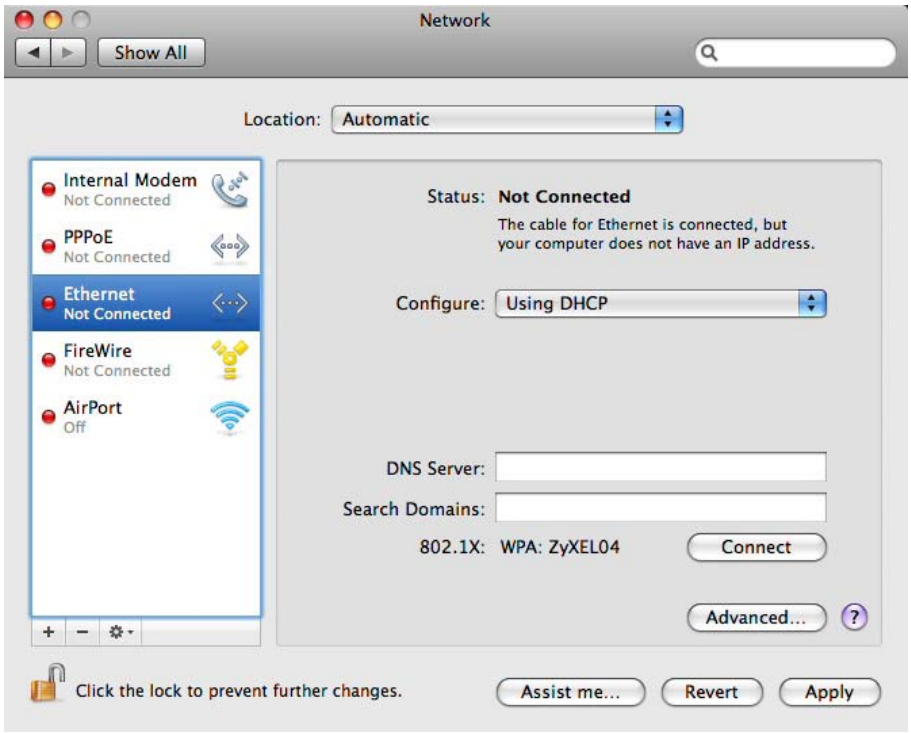
The screens in this section are from Mac OS X 10.5 but can also apply to 10.6.

1 Click **Apple** > **System Preferences**.



2 In **System Preferences**, click the **Network** icon.

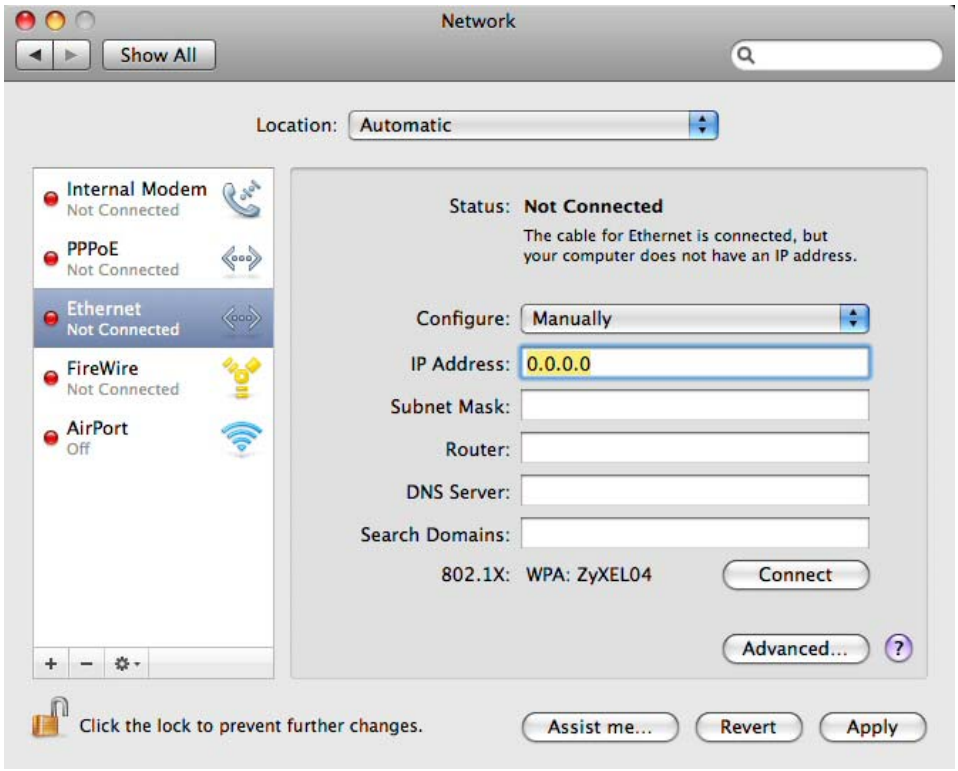
3 When the **Network** preferences pane opens, select **Ethernet** from the list of available connection types.



4 From the **Configure** list, select **Using DHCP** for dynamically assigned settings.

5 For statically assigned settings, do the following:

- From the **Configure** list, select **Manually**.
- In the **IP Address** field, enter your IP address.
- In the **Subnet Mask** field, enter your subnet mask.
- In the **Router** field, enter the IP address of your NBG4115.

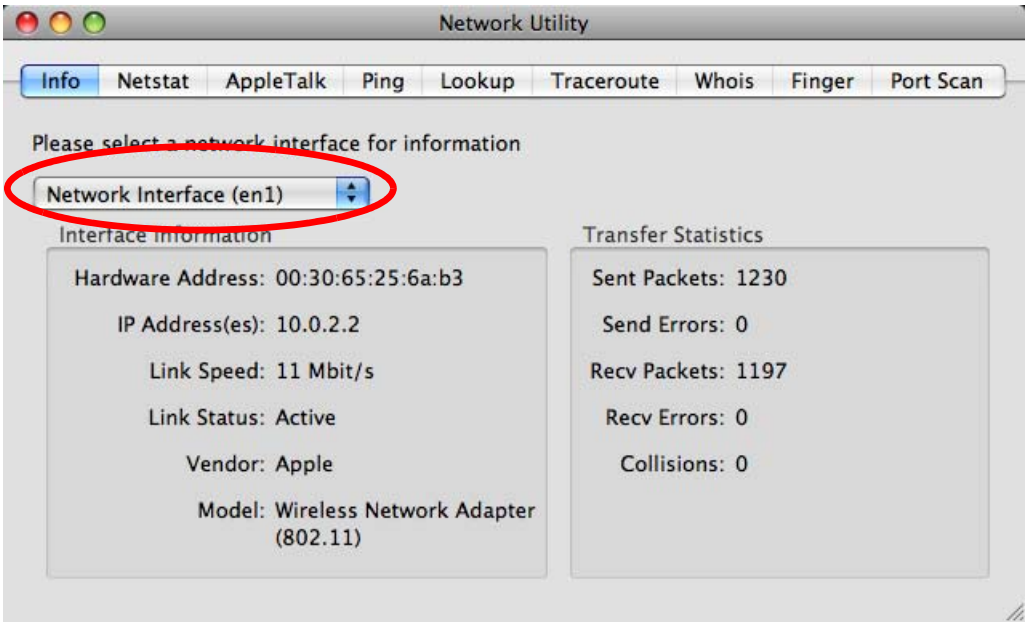


6 Click **Apply** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network interface** from the **Info** tab.

Figure 145 Mac OS X 10.5: Network Utility



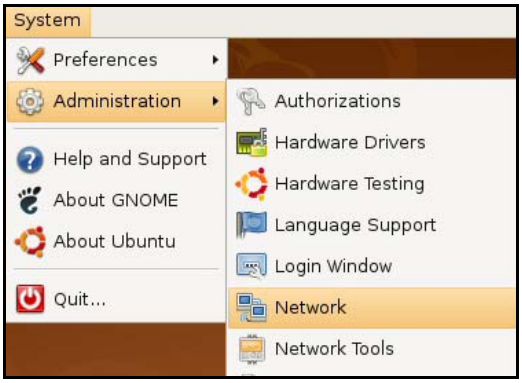
Linux: Ubuntu 8 (GNOME)

This section shows you how to configure your computer's TCP/IP settings in the GNU Object Model Environment (GNOME) using the Ubuntu 8 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default Ubuntu 8 installation.

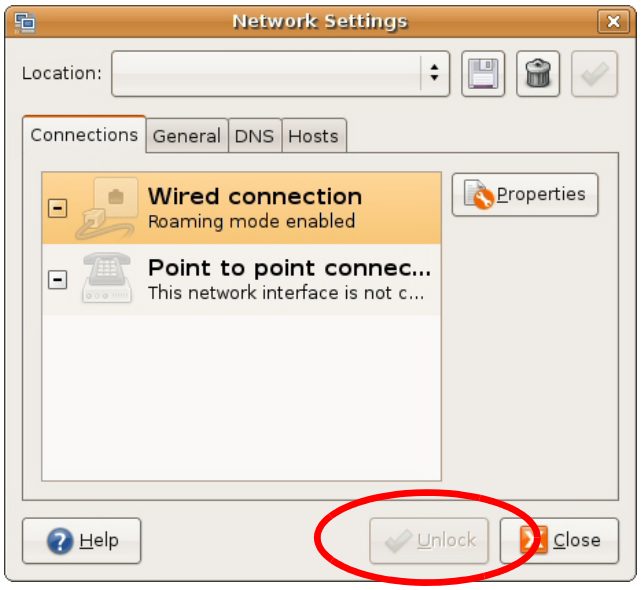
Note: Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in GNOME:

1 Click **System > Administration > Network**.



2 When the **Network Settings** window opens, click **Unlock** to open the **Authenticate** window. (By default, the **Unlock** button is greyed out until clicked.) You cannot make changes to your configuration unless you first enter your admin password.



3 In the **Authenticate** window, enter your admin account name and password then click the **Authenticate** button.

Authenticate
System policy prevents modifying the configuration
An application is attempting to perform an action that requires privileges. Authentication as one of the users below is required to perform this action.
C.J.,,,,, (chris)
Password for chris:
Details
Cancel
Authenticate

4 In the **Network Settings** window, select the connection that you want to configure, then click **Properties**.

5 The **Properties** dialog box opens.

- In the **Configuration** list, select **Automatic Configuration (DHCP)** if you have a dynamic IP address.
- In the **Configuration** list, select **Static IP address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Gateway address** fields.

6 Click **OK** to save the changes and close the **Properties** dialog box and return to the **Network Settings** screen.

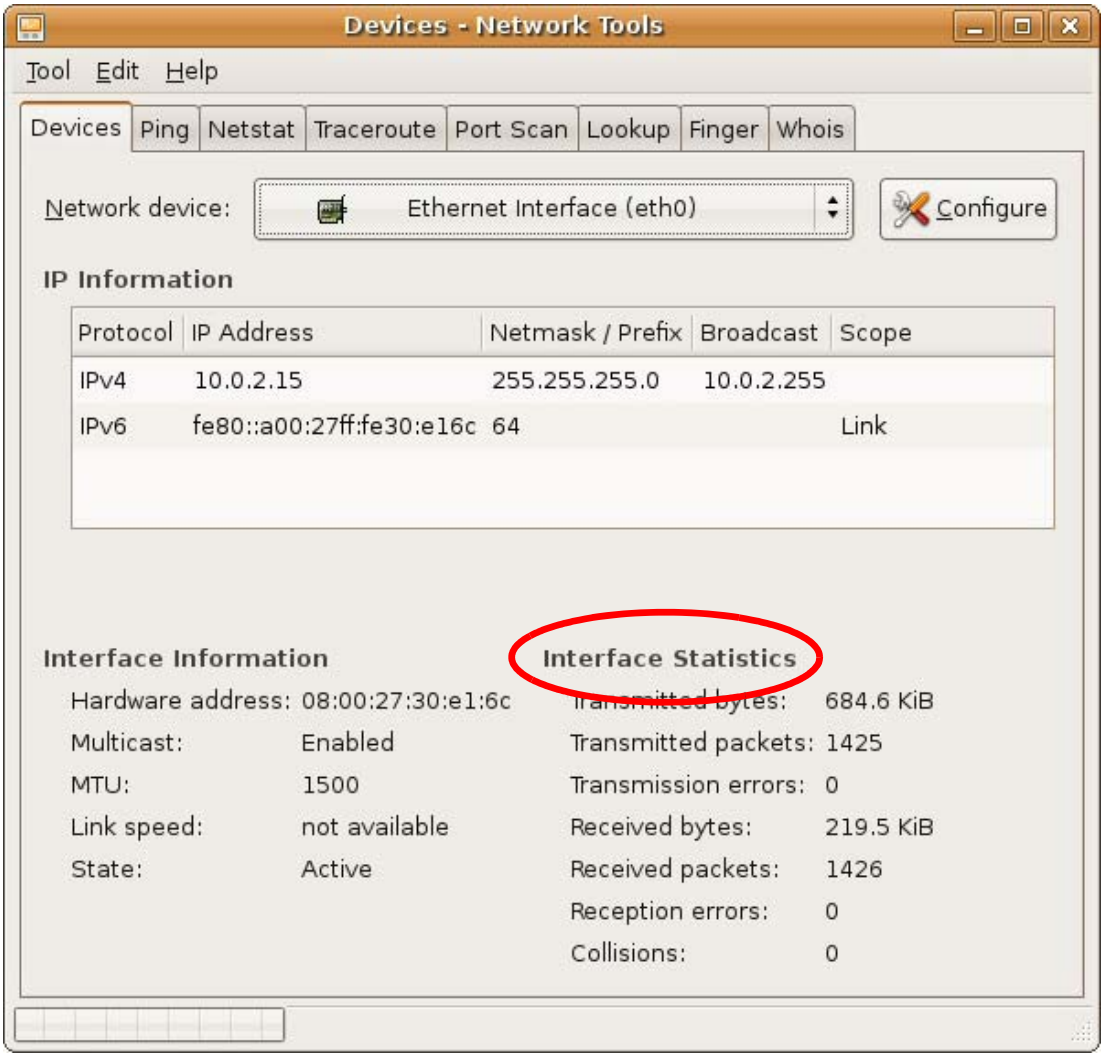
7 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Settings** window and then enter the DNS server information in the fields provided.

8 Click the **Close** button to apply the changes.

Verifying Settings

Check your TCP/IP properties by clicking **System > Administration > Network Tools**, and then selecting the appropriate **Network device** from the **Devices** tab. The **Interface Statistics** column shows data if your connection is working properly.

Figure 146 Ubuntu 8: Network Tools



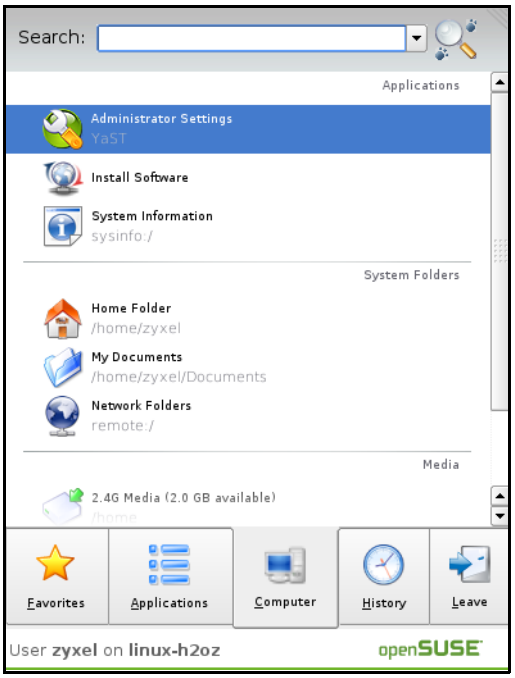
Linux: openSUSE 10.3 (KDE)

This section shows you how to configure your computer's TCP/IP settings in the K Desktop Environment (KDE) using the openSUSE 10.3 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default openSUSE 10.3 installation.

Note: Make sure you are logged in as the root administrator.

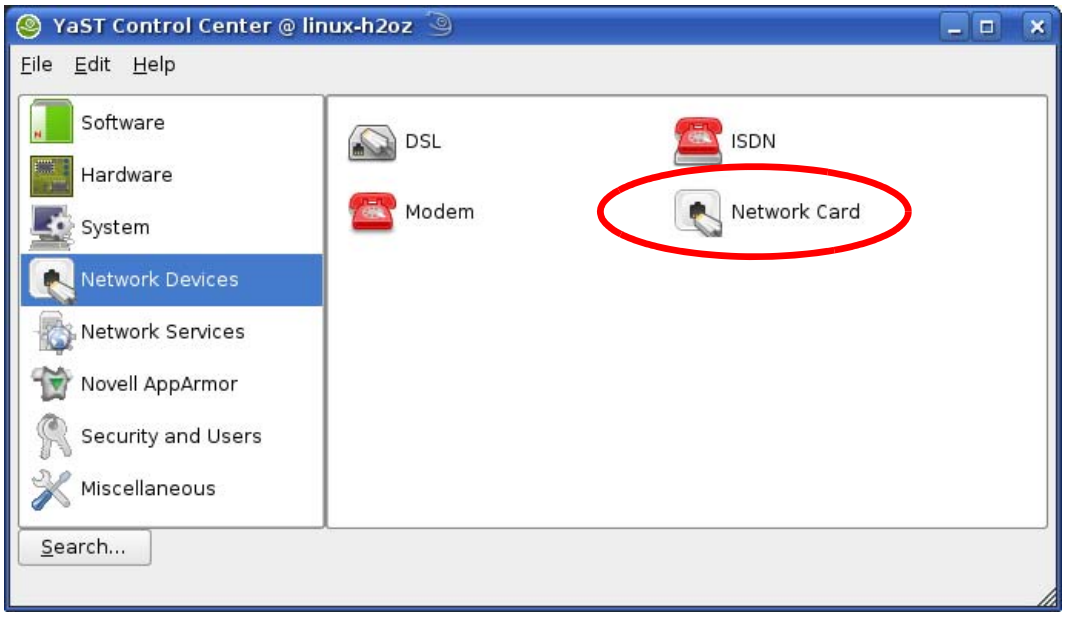
Follow the steps below to configure your computer IP address in the KDE:

1 Click **K Menu > Computer > Administrator Settings (YaST)**.

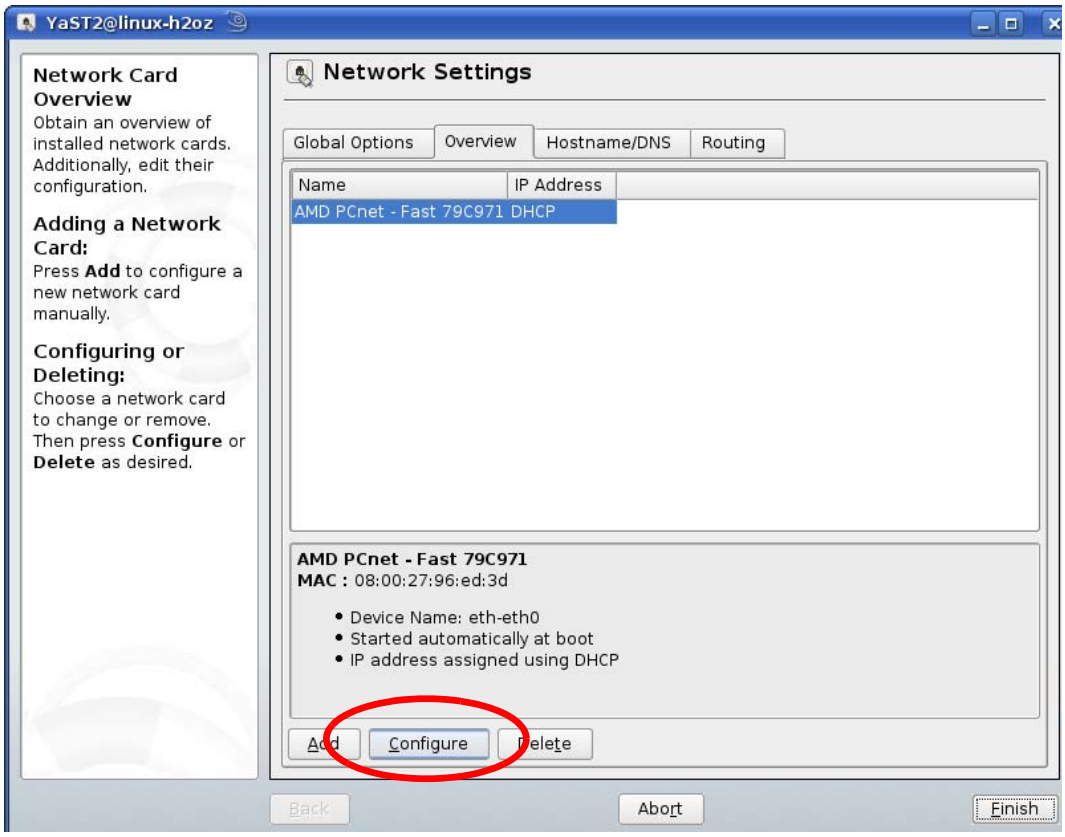


2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.

3 When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.

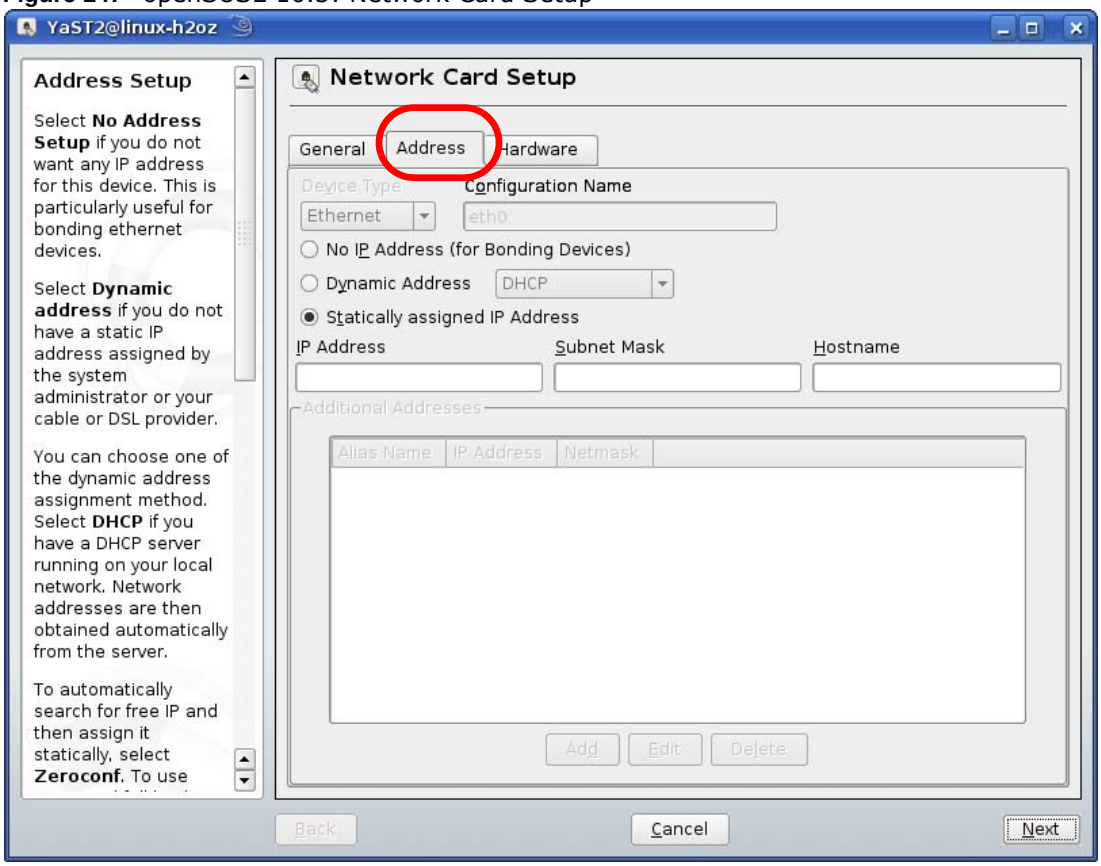


4 When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection **Name** from the list, and then click the **Configure** button.



5 When the **Network Card Setup** window opens, click the **Address** tab

Figure 147 openSUSE 10.3: Network Card Setup

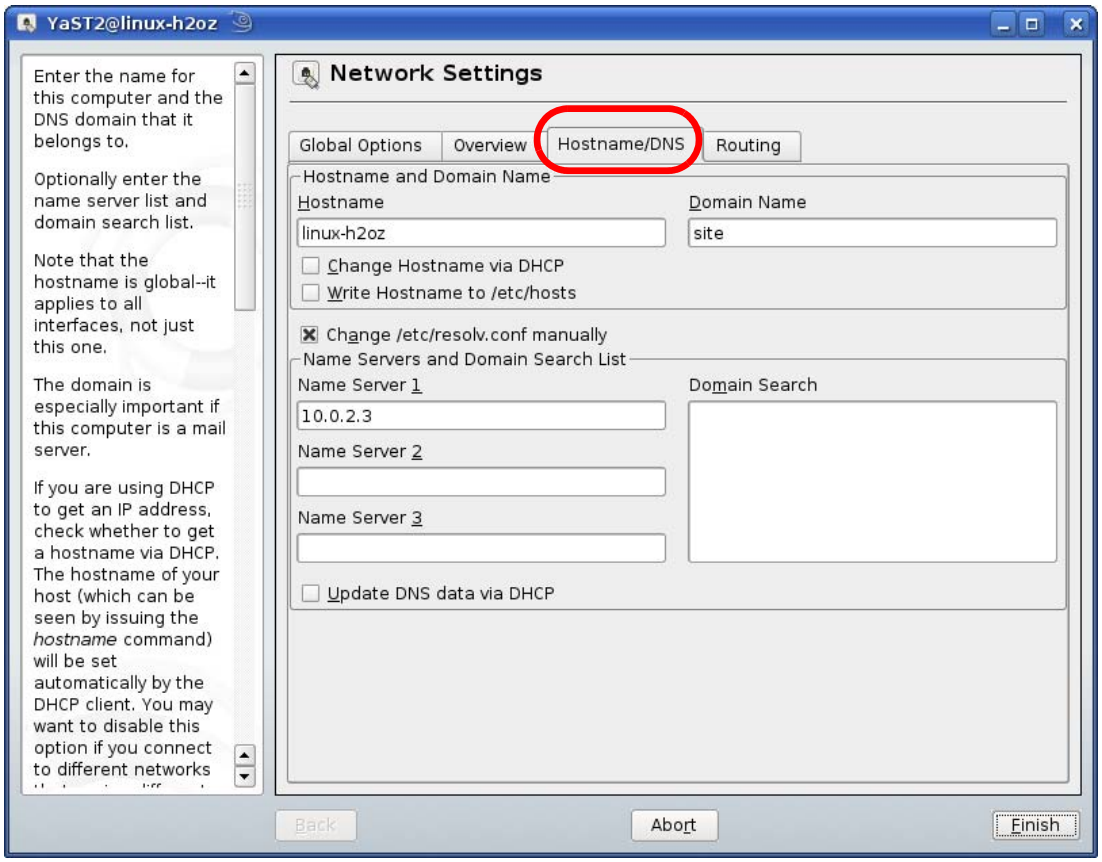

YaST2@linux-h2oz
Address Setup
Select No Address Setup if you do not want any IP address for this device. This is particularly useful for bonding ethernet devices.
Select Dynamic address if you do not have a static IP address assigned by the system administrator or your cable or DSL provider.
You can choose one of the dynamic address assignment method. Select DHCP if you have a DHCP server running on your local network. Network addresses are then obtained automatically from the server.
To automatically search for free IP and then assign it statically, select Zeroconf. To use
Network Card Setup
General
Address
Hardware
Device Type
Configuration Name
Ethernet
eth0
No IP Address (for Bonding Devices)
Dynamic Address
DHCP
Statically assigned IP Address
IP Address
Subnet Mask
Hostname
Additional Addresses
Alias Name
IP Address
Netmask
Add
Edit
Delete
Back
Cancel
Next

6 Select **Dynamic Address (DHCP)** if you have a dynamic IP address.

Select **Statically assigned IP Address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Hostname** fields.

7 Click **Next** to save the changes and close the **Network Card Setup** window.

8 If you know your DNS server IP address(es), click the **Hostname/DNS** tab in **Network Settings** and then enter the DNS server information in the fields provided.

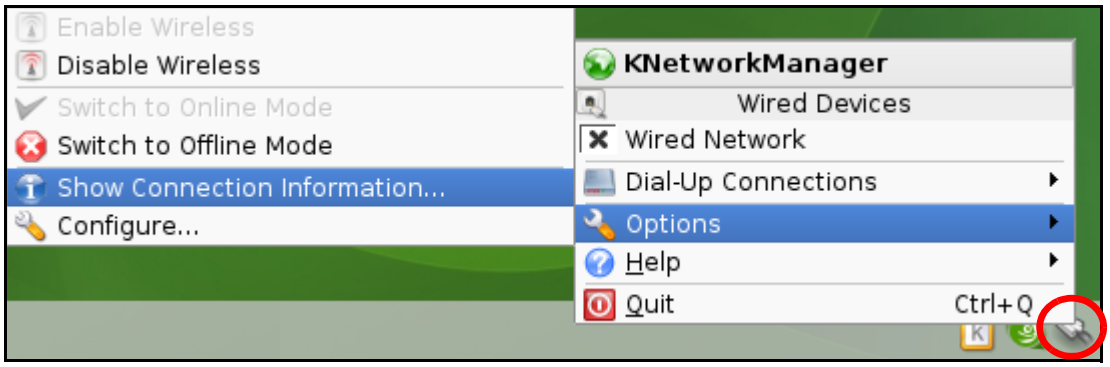

YaST2@linux-h2oz
Enter the name for this computer and the DNS domain that it belongs to.
Optionally enter the name server list and domain search list.
Note that the hostname is global--it applies to all interfaces, not just this one.
The domain is especially important if this computer is a mail server.
If you are using DHCP to get an IP address, check whether to get a hostname via DHCP. The hostname of your host (which can be seen by issuing the hostname command) will be set automatically by the DHCP client. You may want to disable this option if you connect to different networks
Network Settings
Global Options
Overview
Hostname/DNS
Routing
Hostname and Domain Name
Hostname
linux-h2oz
Domain Name
site
Change Hostname via DHCP
Write Hostname to /etc/hosts
Change /etc/resolv.conf manually
Name Servers and Domain Search List
Name Server 1
10.0.2.3
Domain Search
Name Server 2
Name Server 3
Update DNS data via DHCP
Back
Abort
Finish

9 Click **Finish** to save your settings and close the window.

Verifying Settings

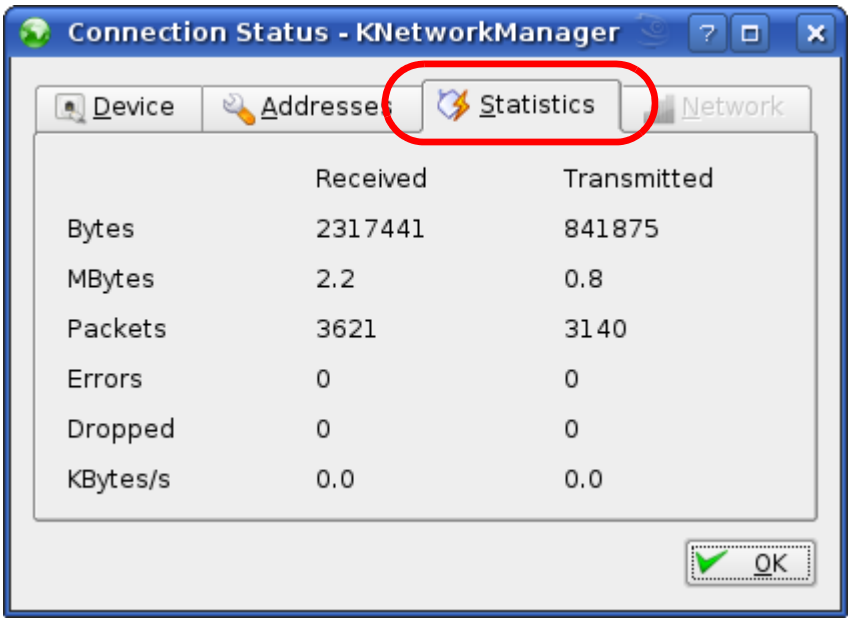
Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

Figure 148 openSUSE 10.3: KNetwork Manager



When the **Connection Status - KNetwork Manager** window opens, click the **Statistics tab** to see if your connection is working properly.

Figure 149 openSUSE: Connection Status - KNetwork Manager



D

Wireless LANs

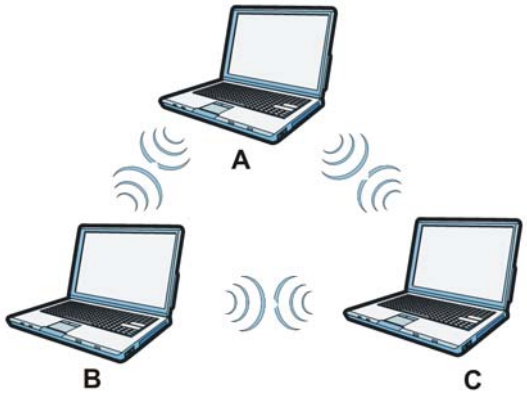
Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an ad-hoc wireless LAN.

Figure 150 Peer-to-Peer Communication in an Ad-hoc Network



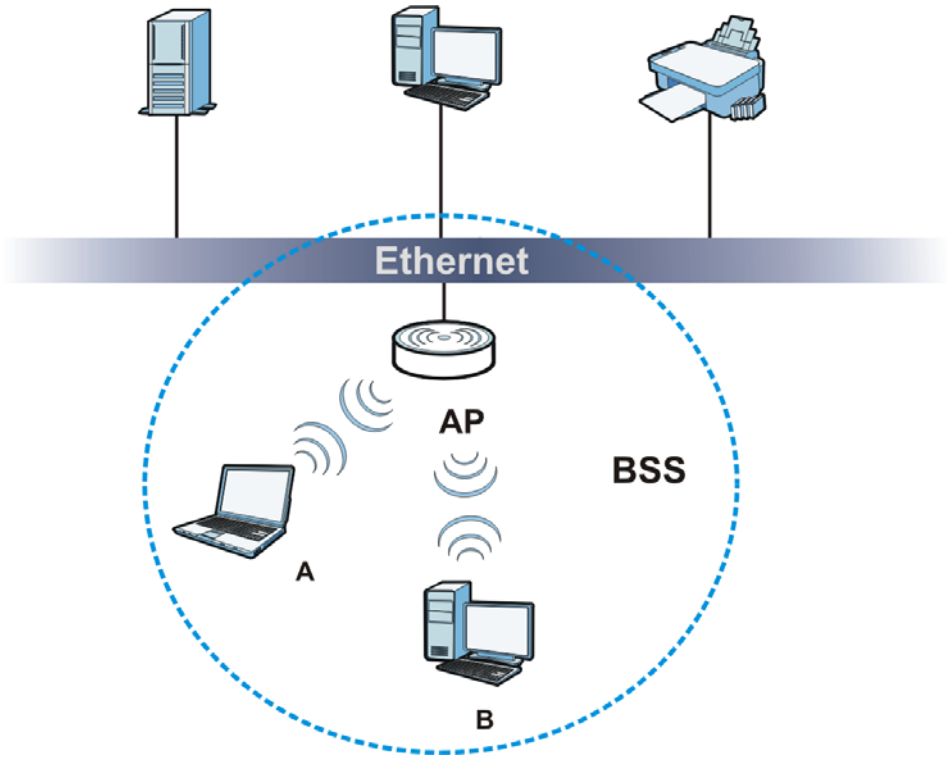
BSS

A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client **A** and **B** can access the wired network and communicate with each other. When Intra-BSS is

disabled, wireless client **A** and **B** can still access the wired network but cannot communicate with each other.

Figure 151 Basic Service Set



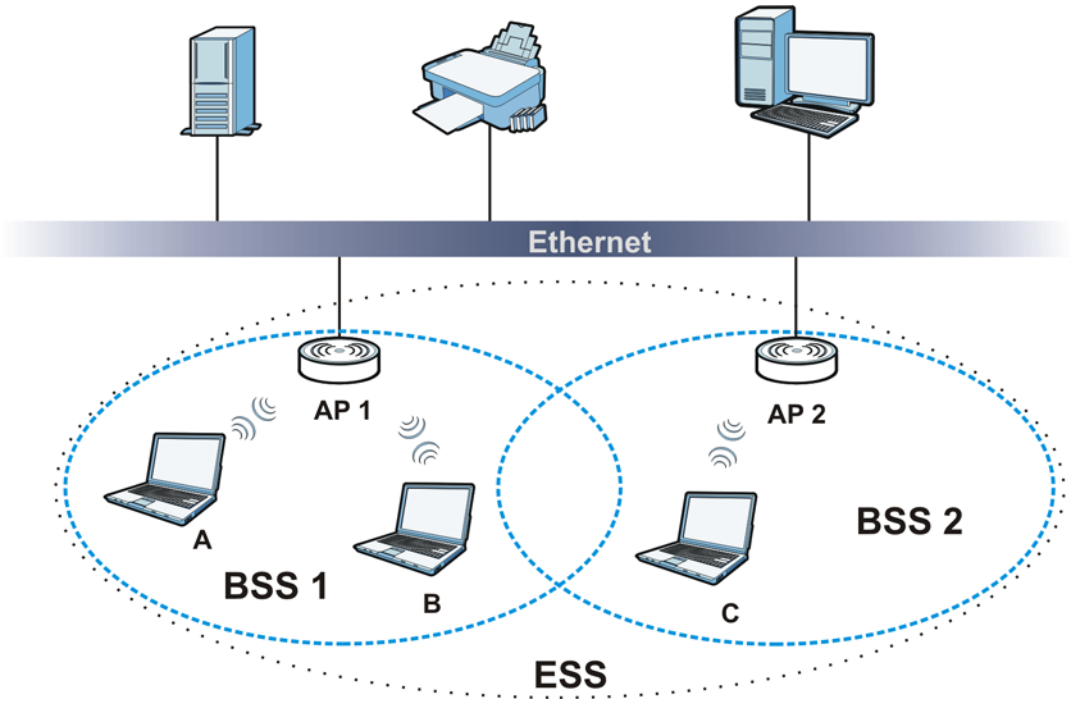
ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless clients within the same ESS must have the same ESSID in order to communicate.

Figure 152 Infrastructure WLAN



Channel

A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

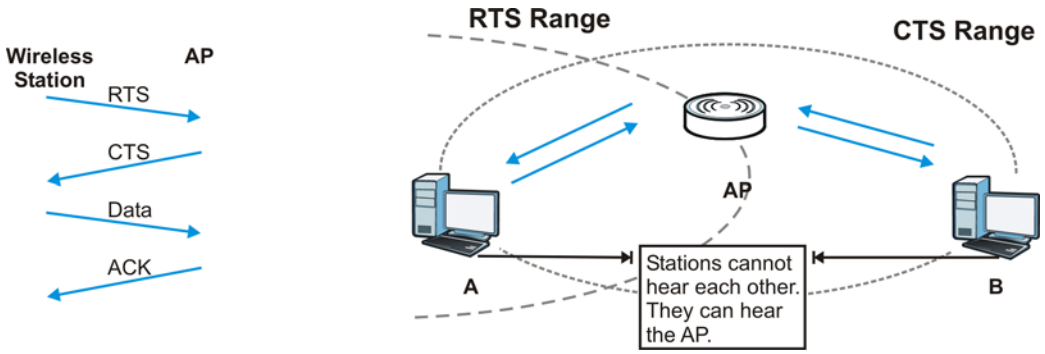
Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they

cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 153 RTS/CTS



When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Preamble Type

Preamble is used to signal that data is coming to the receiver. Short and long refer to the length of the synchronization field in a packet.

Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11 compliant wireless adapters support long preamble, but not all support short preamble.

Use long preamble if you are unsure what preamble mode other wireless devices on the network support, and to provide more reliable communications in busy wireless networks.

Use short preamble if you are sure all wireless devices on the network support it, and to provide more efficient communications.

Use the dynamic setting to automatically use short preamble when all wireless devices on the network support it, otherwise the NBG4115 uses long preamble.

Note: The wireless devices MUST use the same preamble mode in order to communicate.

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 87 IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless clients, access points and the wired network.

Wireless security methods available on the NBG4115 are data encryption, wireless client authentication, restricting access by device MAC address and hiding the NBG4115 identity.

The following figure shows the relative effectiveness of these wireless security methods available on your NBG4115.

Table 88 Wireless Security Levels

SECURITY LEVEL	SECURITY TYPE
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
	Wi-Fi Protected Access (WPA)
	WPA2
Most Secure	

Note: You must enable the same wireless security settings on the NBG4115 and on all wireless clients that you want to associate with it.

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication

  Determines the identity of the users.
- Authorization

  Determines the network services available to authenticated users once they are connected to the network.
- Accounting

  Keeps track of the client’s network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless client and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request

  Sent by an access point requesting authentication.
- Access-Reject

  Sent by a RADIUS server rejecting access.
- Access-Accept

  Sent by a RADIUS server allowing access.
- Access-Challenge

  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request

  Sent by the access point requesting accounting.
- Accounting-Response

  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x. .

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless client. The wireless client 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the wireless security configuration screen. You may still configure and store keys, but they will not be used while dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 89 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA2 also uses TKIP when required for compatibility reasons, but offers stronger encryption than TKIP with Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP).

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm

called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a Wi-Fi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it’s still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP)

User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

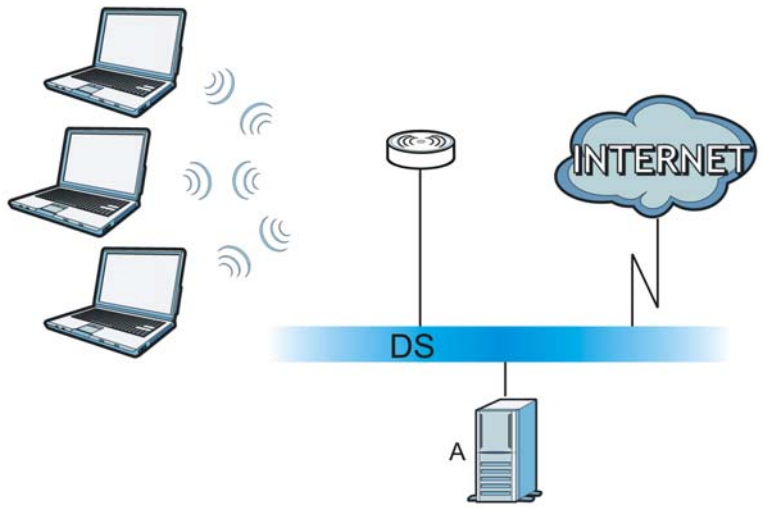
The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

WPA(2) with RADIUS Application Example

To set up WPA(2), you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

1. The AP passes the wireless client's authentication request to the RADIUS server.
2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
3. A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.
4. The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 154 WPA(2) with RADIUS Application Example



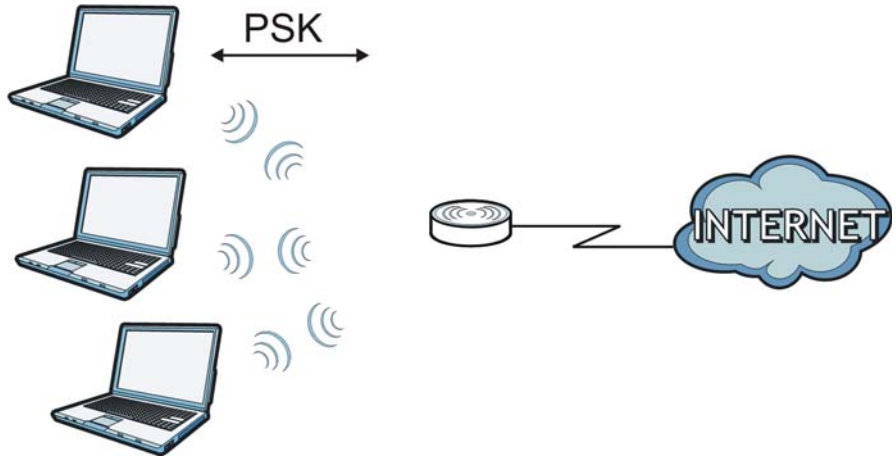
WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

1. First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).
2. The AP checks each wireless client's password and allows it to join the network only if the password matches.
3. The AP and wireless clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.

4 The AP and wireless clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

Figure 155 WPA(2)-PSK Authentication



Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method or key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 90 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP/AES	No	Enable
WPA-PSK	TKIP/AES	Yes	Disable
WPA2	TKIP/AES	No	Enable
WPA2-PSK	TKIP/AES	Yes	Disable

Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b and IEEE 802.11g) or 5GHz (IEEE 802.11a) is needed to communicate efficiently in a wireless LAN

Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas for WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to–point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

E

Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 91 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.

Table 91 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/ server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Management Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/ server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.

Table 91 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

F

Legal Information

Copyright

Copyright © 2012 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Certifications

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device has been designed for the WLAN 2.4 GHz network throughout the EC region and Switzerland, with restrictions in France.

Ce produit est conçu pour les bandes de fréquences 2,4 GHz conformément à la législation Européenne. En France métropolitaine, suivant les décisions n°03-908 et 03-909 de l'ARCEP, la puissance d'émission ne devra pas dépasser 10 mW (10 dB) dans le cadre d'une installation WiFi en extérieur pour les fréquences comprises entre 2454 MHz et 2483,5 MHz.

Viewing Certifications

Go to http://www.zyxel.com to view this product’s documentation and certifications.

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

注意 ！

依據　低功率電波輻射性電機管理辦法

第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。
減少電磁波影響，請妥適使用。

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized ZyXEL local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any

implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at www.zyxel.com. To obtain the source code covered under those Licenses, please contact support@zyxel.com.tw to get it.

Regulatory Information

European Union

The following information applies if you use the product within the European Union.

Declaration of Conformity with Regard to EU Directive 1999/5/EC (R&TTE Directive)

Compliance Information for 2.4GHz and 5GHz Wireless Products Relevant to the EU and Other Countries Following the EU Directive 1999/5/EC (R&TTE Directive)

[Czech]	ZyXEL tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/EC.
[Danish]	Undertegnede ZyXEL erklærer herved, at følgende udstyr udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
[German]	Hiermit erklärt ZyXEL, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EU befindet.
[Estonian]	Käesolevaga kinnitab ZyXEL seadme seadmed vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, ZyXEL declares that this equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
[Spanish]	Por medio de la presente ZyXEL declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
[Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ ZyXEL ΔΗΛΩΝΕΙ ΟΤΙ εξοπλισμός ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕC.
[French]	Par la présente ZyXEL déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/EC.
[Italian]	Con la presente ZyXEL dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
[Latvian]	Ar šo ZyXEL deklarē, ka iekārtas atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
[Lithuanian]	Šiuo ZyXEL deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
[Dutch]	Hierbij verklaart ZyXEL dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EC.
[Maltese]	Hawnhekk, ZyXEL, jiddikjara li dan tagħmir jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
[Hungarian]	Alulírott, ZyXEL nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EK irányelv egyéb elõírásainak.
[Polish]	Niniejszym ZyXEL oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.

[Portuguese]	ZyXEL declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/EC.
[Slovenian]	ZyXEL izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/EC.
[Slovak]	ZyXEL týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/EC.
[Finnish]	ZyXEL vakuuttaa täten että laitteet tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
[Swedish]	Härmed intygar ZyXEL att denna utrustning står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EC.
[Bulgarian]	С настоящото ZyXEL декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 1999/5/EC.
[Icelandic]	Hér með lýsir, ZyXEL því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 1999/5/EC.
[Norwegian]	Erklærer herved ZyXEL at dette utstyret er I samsvar med de grunnleggende kravene og andre relevante bestemmelser I direktiv 1999/5/EF.
[Romanian]	Prin prezenta, ZyXEL declară că acest echipament este în conformitate cu cerinţele esenţiale şi alte prevederi relevante ale Directivei 1999/5/EC.

National Restrictions

This product may be used in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Ce produit peut être utilisé dans tous les pays de l'UE (et dans tous les pays ayant transposés la directive 1999/5/CE) sans aucune limitation, excepté pour les pays mentionnés ci-dessous:

Questo prodotto è utilizzabile in tutte i paesi EU (ed in tutti gli altri paesi che seguono le direttive EU 1999/5/EC) senza nessuna limitazione, eccetto per i paesii menzionati di seguito:

Das Produkt kann in allen EU Staaten ohne Einschränkungen eingesetzt werden (sowie in anderen Staaten die der EU Direktive 1995/5/CE folgen) mit Außnahme der folgenden aufgeführten Staaten:

In the majority of the EU and other European countries, the 2, 4- and 5-GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries inwhich additional restrictions or requirements or both are applicable.

The requirements for any country may evolve. ZyXEL recommends that you check with the local authorities for the latest status of their national regulations for both the 2,4- and 5-GHz wireless LANs.

The following countries have restrictions and/or requirements in addition to those given in the table labeled "*Overview of Regulatory Requirements for Wireless LANs*":.

Overview of Regulatory Requirements for Wireless LANs			
Frequency Band (MHz)	Max Power Level (EIRP)[1] (mW)	Indoor ONLY	Indoor and Outdoor
2400-2483.5	100		V
5150-5350	200	V	
5470-5725	1000		V

Belgium

The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check http://www.bipt.be for more details.

Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie http://www.bipt.be voor meer gegevens.

Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez http://www.ibpt.be pour de plus amples détails.

Denmark

In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage.

I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.

France

For 2.4 GHz, the output power is restricted to 10 mW EIRP when the product is used outdoors in the band 2454 - 2483.5 MHz. There are no restrictions when used indoors or in other parts of the 2.4 GHz band. Check http://www.arcep.fr/ for more details.

Pour la bande 2.4 GHz, la puissance est limitée à 10 mW en p.i.r.e. pour les équipements utilisés en extérieur dans la bande 2454 - 2483.5 MHz. Il n'y a pas de restrictions pour des utilisations en intérieur ou dans d'autres parties de la bande 2.4 GHz. Consultez http://www.arcep.fr/ pour de plus amples détails.

R&TTE 1999/5/EC		
WLAN 2.4 – 2.4835 GHz		
IEEE 802.11 b/g/n		
Location	Frequency Range(GHz)	Power (EIRP)
Indoor (No restrictions)	2.4 – 2.4835	100mW (20dBm)
Outdoor	2.4 – 2.454	100mW (20dBm)
	2.454 – 2.4835	10mW (10dBm)

Italy

This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check http://www.sviluppoeconomico.gov.it/ for more details.

Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all 'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare http://www.sviluppoeconomico.gov.it/ per maggiori dettagli.

Latvia

The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check http://www.esd.lv for more details.

2.4 GHz frekvenèu joslas izmantoðanai ârpus telpâm nepieciešama atïauja no Elektronisko sakaru direkcijas. Vairâk informâcijas: http://www.esd.lv.

Notes:

1. Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 1999/5/EC has also been implemented in those countries.

2. The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used(specified in dBi) to the output power available at the connector (specified in dBm).

List of national codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Malta	MT
Belgium	BE	Netherlands	NL
Cyprus	CY	Poland	PL
Czech Republic	CR	Portugal	PT
Denmark	DK	Slovakia	SK
Estonia	EE	Slovenia	SI
Finland	FI	Spain	ES
France	FR	Sweden	SE
Germany	DE	United Kingdom	GB
Greece	GR	Iceland	IS
Hungary	HU	Liechtenstein	LI
Ireland	IE	Norway	NO
Italy	IT	Switzerland	CH
Latvia	LV	Bulgaria	BG
Lithuania	LT	Romania	RO
Luxembourg	LU	Turkey	TR

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the power outlet.

- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.

Index

A

Address Assignment 98
Advanced Encryption Standard
  See AES.
AES 251
alternative subnet mask notation 207
antenna
  directional 255
  gain 255
  omni-directional 255
AP 15
AP (access point) 245
AP Mode
  menu 58
  overview 55
  status screen 56
AP+Bridge 15
Auto-bridge 111

B

Backup configuration 178
Bandwidth management
  overview 146
  priority 151
  services 152
Basic Service Set, See BSS 243
BitTorrent 153
Bridge/Repeater 15
BSS 243

C

CA 250
Certificate Authority
  See CA.
certifications
  notices 261
  viewing 261
Channel 33, 57
channel 78, 245
  interference 245
Configuration
  backup 178
  reset the factory defaults 179
  restore 178
content filtering 139
  by keyword (in URL) 139
copyright 261
CPU usage 33, 57
CTS (Clear to Send) 246

D

Daylight saving 172
DDNS
  service providers 133
DHCP 37, 117
  DHCP server
  see also Dynamic Host Configuration Protocol
DHCP client information 120
DHCP client list 120
DHCP server 114, 117
DHCP table 37, 120
  DHCP client information
  DHCP status
disclaimer 261
DNS 51, 119
  DNS server
  see also Domain name system
DNS Server 98
DNS server 119
documentation
  related 2
Domain name 42
  vs host name. see also system name

Domain Name System 119
Domain Name System. See DNS.
duplex setting 34, 57
Dynamic DNS 133
Dynamic Host Configuration Protocol 117
dynamic WEP key exchange 250
DynDNS 133
DynDNS see also DDNS 133

E

EAP Authentication 249
e-mail 91
encryption 79, 251
  and local (user) database 80
  key 80
  WPA compatible 80
ESS 244
ESSID 189
Extended Service Set, See ESS 244
Extended wireless security 44

F

Factory LAN defaults 117, 118
FCC interference statement 261
File Transfer Program 152
Firewall 136
  Firewall overview
  guidelines 136
  ICMP packets 137
  network security
  Stateful inspection 136
  ZyXEL device firewall 136
firewall
  stateful inspection 135
Firmware upload 176
  file extension
  using HTTP
firmware version 33, 57
fragmentation threshold 246
FTP. see also File Transfer Program 152

G

gateway 144
General wireless LAN screen 80
Guide
  Quick Start 2

H

hidden node 245
HTTP 152
Hyper Text Transfer Protocol 152

I

IANA 212
IBSS 243
IEEE 802.11g 247
IGMP 99
  see also Internet Group Multicast Protocol
  version
IGMP version 99
Independent Basic Service Set
  See IBSS 243
initialization vector (IV) 252
Install UPnP
  Windows XP 158
Internet Assigned Numbers Authority
  See IANA 212
Internet connection
  Ethernet
  PPPoE. see also PPP over Ethernet
  PPTP
  WAN connection
Internet connection wizard 45
Internet Group Multicast Protocol 99
IP Address 114, 126
IP address 51
  dynamic
IP Pool 118

L

LAN 113
IP pool setup 117
LAN overview 113
LAN setup 113
LAN TCP/IP 118
Language 184
Link type 34, 57
local (user) database 79
and encryption 80
Local Area Network 113

M

MAC 86
MAC address 78, 98
cloning 53, 98
MAC address filter 78
MAC address filtering 86
MAC filter 86
managing the device
good habits 16
using the web configurator. See web configurator.
using the WPS. See WPS.
MBSSID 15
Media access control 86
Memory usage 33, 57
Message Integrity Check (MIC) 251
Metric 145
mode 15
Multicast 99
IGMP 99

N

NAT 123, 126, 212
global 124
how it works 125
inside 124
local 124
outside 124
overview 123
port forwarding 130
see also Network Address Translation
server 124
server sets 130
NAT traversal 156
Navigation Panel 35, 58
navigation panel 35, 58
NetBIOS 99
see also Network Basic Input/Output System 99
Network Address Translation 123, 126

O

Operating Channel 33, 57
operating mode 15
other documentation 2

P

P2P 153
Pairwise Master Key (PMK) 252, 253
peer-to-peer 153
Point-to-Point Protocol over Ethernet 46, 104
Point-to-Point Tunneling Protocol 47, 106
Pool Size 118
Port forwarding 126, 130
default server 130
example 130
local server 126
port numbers
services
port speed 34, 57
PPPoE 46, 104
benefits 46
dial-up connection
see also Point-to-Point Protocol over Ethernet 46
PPTP 47, 106
see also Point-to-Point Tunneling Protocol 47
preamble mode 247
product registration 263
PSK 252

Q

Quality of Service (QoS) 89
Quick Start Guide 2

R

RADIUS 248
  message types 249
  messages 249
  shared secret key 249
RADIUS server 79
registration
  product 263
related documentation 2
Remote management 154
  and NAT 154
  limitations 154
  system timeout 155
Reset button 31, 179
Reset the device 31
Restore configuration 178
Roaming 87
RTS (Request To Send) 246
  threshold 245, 246
RTS/CTS Threshold 77, 87

S

safety warnings 266
Scheduling 94
Service and port numbers 153
Service Set 81
Service Set IDentification 81
Service Set IDentity. See SSID.
Session Initiated Protocol 153
SIP 153
SSID 33, 57, 78, 81
stateful inspection firewall 135
Static DHCP 119
Static Route 144
Status 31
subnet 205
Subnet Mask 114
subnet mask 51, 206
subnetting 208
Summary
  DHCP table 37
  Packet statistics 38
  Wireless station status 38
Sys Op Mode 181
System General Setup 169
System Name 170
System name 42
  vs computer name
System restart 180

T

TCP/IP configuration 117
Temporal Key Integrity Protocol (TKIP) 251
Time setting 171
trigger port 131
Trigger port forwarding 131
  example 131
  process 131

U

Universal Plug and Play 156
  application 156
UPnP 156
  security issues 157
URL Keyword Blocking 140
user authentication 79
  local (user) database 79
  RADIUS server 79

V

VoIP 153
VPN 106

W

WAN
  IP address assignment 50
WAN (Wide Area Network) 97
WAN advanced 110
WAN IP address 50
WAN IP address assignment 52
WAN MAC address 98
warranty 262
  note 262
Web Configurator
  how to access 29
  Overview 29
Web configurator
  navigating 31
web configurator 16
WEP Encryption 84
WEP encryption 83
WEP key 83
Wi-Fi Protected Access 251
Wireless association list 38
wireless channel 189
wireless client WPA supplicants 252
wireless LAN 189
wireless LAN scheduling 94
Wireless LAN wizard 43
Wireless network
  basic guidelines 77
  channel 78
  encryption 79
  example 77
  MAC address filter 78
  overview 77
  security 78
  SSID 78
Wireless security 78
  overview 78
  type 78
wireless security 189, 247
Wireless tutorial 55, 65
Wizard setup 41
  complete 54
  Internet connection 45
  system information 42
  wireless LAN 43
WLAN
  interference 245
  security parameters 254
World Wide Web 152
WPA 251
  key caching 252
  pre-authentication 252
  user authentication 252
  vs WPA-PSK 252
  wireless client supplicant 252
  with RADIUS application example 253
WPA compatible 80
WPA2 251
  user authentication 252
  vs WPA2-PSK 252
  wireless client supplicant 252
  with RADIUS application example 253
WPA2-Pre-Shared Key 251
WPA2-PSK 251, 252
  application example 253
WPA-PSK 251, 252
  application example 253
WPS 15
WWW 91, 152

X

Xbox Live 153